服务器配置与应用
（Windows Server 2008 R2）
（第3版）

柴方艳　主　编

张灵光　薛　刚　副主编

電子工業出版社

Publishing House of Electronics Industry

北京・BEIJING

内 容 简 介

本书以目前性能稳定并广泛使用的 Windows 系列网络操作系统 Windows Server 2008 R2 为平台，全面介绍了网络服务器搭建、管理及常用服务配置方法与技巧。内容选取依据企业网络建设背景，由简单到复杂，分析具体项目需求，提炼出 14 个网络运维管理项目，涵盖了 Windows Server 2008 R2 的安装、配置、管理及各种网络服务功能的搭建和安全功能的实现。通过本书的学习，读者可顺利完成中小企业局域网常见服务器的管理与配置。本书注重职业能力和实践技能的培养，内容结构采用项目式，设计了多个典型工作任务，步骤清晰，图文并茂，突出实用性和实践性。

本书既可作为高职高专类院校计算机专业的教材，也可作为相关人员的计算机网络培训教材，还可作为从事网络管理的专业人员及网络爱好者的参考书。

图书在版编目（CIP）数据

服务器配置与应用：Windows Server 2008 R2 / 柴方艳主编．—3 版．—北京：电子工业出版社，2018.4
ISBN 978-7-121-33862-5

Ⅰ. ①服… Ⅱ. ①柴… Ⅲ. ①网络服务器－配置 Ⅳ. ①TP368.5

中国版本图书馆 CIP 数据核字(2018)第 050438 号

策划编辑：宋　梅
责任编辑：宋　梅
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：16.75　　字数：429 千字
版　　次：2012 年 6 月第 1 版
　　2018 年 4 月第 3 版
印　　次：2018 年 4 月第 1 次印刷
定　　价：49.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：mariams@phei.com.cn。

前　言

Windows Server 2008 R2 是稳定的 64 位 Windows Server 操作系统，与之前的版本相比提升了系统管理弹性、网络存取方式和在信息安全等领域的应用，为企业提供了一个安全、可靠、易于管理的高效服务平台。

本书以具体信息技术企业的网络需求为任务主线，全面介绍了 Windows Server 2008 R2 系统管理与网络服务配置方法，其内容涵盖 Windows Server 2008 R2 的安装与网络环境设置、本地用户和组的管理、NTFS 文件系统的应用与文件服务器的配置、域网络搭建、域环境管理、磁盘管理、常用网络服务、虚化化服务、远程桌面部署、备份与还原等。

本书共 14 章，内容结构采用项目式，共包含 14 个网络运维管理项目，在每个项目中先分析项目需求，然后提供完成这个项目需要掌握的相关知识，再将项目分解为多个工作任务，分别介绍为完成任务而采取的详细步骤。各项目均设置实训部分和习题部分，实训部分针对读者所学习的知识进行进一步领悟和简单运用，以达到吸收和转化的目的。案例的选取力求还原真实岗位工作需求，使读者可以轻松、愉快地完成学习过程。全书内容具体安排如下：

第 1 章　介绍网络管理模式及 Windows Server 2008 版本，通过 2 个工作任务详细说明 Windows Server 2008 R2 的安装过程以及 Windows Server 2008 R2 的初始化配置。

第 2 章　介绍 Windows 网络组件和网络测试工具，通过 2 个工作任务详细说明本地用户和组的管理。

第 3 章　介绍 NTFS 文件系统的作用、文件和文件夹的 NTFS 权限，通过 4 个工作任务详细说明文件服务器和打印服务器的配置过程。

第 4 章　介绍活动目录和域的相关知识，通过 5 个工作任务详细说明域环境网络的部署以及在域环境下用户、组和组织单位的管理与应用。

第 5 章　介绍本地安全策略和组策略的内容和作用，通过 4 个工作任务详细说明应用组策略实现用户环境控制、组策略应用规则和软件部署方法。

第 6 章　介绍磁盘类型、磁盘分区和磁盘配额相关知识，通过 3 个工作任务详细说明动态磁盘的创建过程与磁盘配额的使用方法。

第 7 章　介绍 DHCP 租约过程、更新与释放 IP 租约的方法，通过 3 个工作任务详细说明 DHCP 服务器及客户机配置和维护的方法。

第 8 章　介绍 DNS 域名空间和域名查询模式相关知识，通过 3 个工作任务详细说明配置 DNS 服务器、DNS 客户机及维护 DNS 服务器的过程。

第 9 章　介绍 IIS 与 WWW 服务的相关知识，通过 5 个工作任务详细说明运用 IIS 建立及配置 Web 服务器和 FTP 服务器的过程。

第 10 章　介绍远程访问服务的应用背景及相关协议，通过 2 个工作任务详细说明远程访问服务器的搭建过程以及使用网络策略控制远程访问的方法。

第 11 章　介绍公钥加密技术、PKI 协议和证书颁发机构等相关知识，通过 2 个工作任务说明证书服务器的配置过程和网站证书的应用。

第 12 章　介绍远程桌面终端和主机的相关知识，通过 2 个工作任务说明远程桌面服务器部署方法和 RemoteApp 的应用。

第 13 章　介绍服务器虚拟化相关知识，通过 4 个工作任务说明虚拟机的创建与管理方法。

第 14 章　介绍 Windows 备份工具和高级启动选项，通过 2 个工作任务说明备份与还原数据的方法及 Windows 安全模式的应用。

本书内容全面、结构清晰、图文并茂，所有操作可按照实际屏幕截图分步骤进行，读者可以边看书边上机操作，通过具体操作，更好地理解基本知识。本书的基础知识介绍所占篇幅较少，充分体现以应用技术为重点，尽量避免讲解高难度的专业理论，使读者更容易上手。

本书由黑龙江农业经济职业学院柴方艳担任主编并负责全书的统稿工作，新疆农业职业技术学院张灵光和大庆职业学院薛刚担任副主编。其中，第 8、9、10、12、13 章由柴方艳编写，第 1、2 章由张灵光编写，第 3、14 章由薛刚编写，第 5、11 章由黑龙江农业经济职业学院庄伟编写，第 4、6、7 章由黑龙江农业经济职业学院邵丹编写。

本书既可作为高职高专类院校计算机专业的教材，也可作为相关人员的计算机网络培训教材，还可作为从事网络管理的专业人员及网络爱好者的参考书。

由于编者水平有限，书中不当之处，恳请广大读者指正。E-mail: cfy231@126.com。

本教材配套有教学资源 PPT 课件，如有需要，请登录电子工业出版社华信教育资源网（www.hxedu.com.cn），注册后免费下载。

编　著　者

2018 年 3 月

目　　录

第 1 章　Windows Server 2008 R2 安装 …… 1

1.1　知识介绍——客户机与服务器 …… 2
1.2　知识介绍——Windows Server 2008 R2 版本 …… 3
1.3　任务 1：安装 Windows Server 2008 R2 …… 4
1.3.1　硬件配置及安装类型 …… 4
1.3.2　安装步骤 …… 5
1.4　任务 2：Windows Server 2008 R2 基本配置 …… 7
1.4.1　初始配置 …… 8
1.4.2　添加角色 …… 8
1.4.3　添加功能 …… 9
1.5　实训 …… 10
1.6　习题 …… 10

第 2 章　配置网络与工作组环境 …… 11

2.1　知识介绍——Windows 网络组件与 IP 地址 …… 12
2.1.1　Windows 网络组件 …… 12
2.1.2　网络参数 …… 12
2.2　知识介绍——网络测试工具与计算机名称 …… 15
2.2.1　网络测试工具 …… 15
2.2.2　计算机名称与工作组 …… 17
2.3　任务 1：创建与管理本地用户账户 …… 19
2.3.1　创建本地用户账户 …… 19
2.3.2　设置账户属性 …… 20
2.3.3　修改和删除用户账户 …… 21
2.4　任务 2：创建与管理本地组 …… 22
2.5　实训 …… 23
2.6　习题 …… 24

第 3 章　文件和打印服务器 …… 25

3.1　知识介绍——NTFS 权限 …… 26
3.1.1　NTFS 权限概述 …… 26
3.1.2　文件和文件夹权限 …… 27
3.2　任务 1：应用 NTFS 权限 …… 27
3.2.1　简单应用 …… 27

3.2.2 权限的组合 ····· 28
3.2.3 权限的继承 ····· 29
3.2.4 权限的拒绝 ····· 30
3.2.5 用户的最终有效权限 ····· 31
3.2.6 取得所有权 ····· 32
3.2.7 移动和复制对权限的影响 ····· 34
3.3 任务 2：访问网络文件 ····· 35
3.3.1 公用文件夹 ····· 35
3.3.2 新建共享文件夹 ····· 36
3.3.3 访问共享文件夹 ····· 38
3.3.4 隐藏共享文件夹 ····· 41
3.4 任务 3：设置共享权限 ····· 42
3.5 任务 4：安装和配置打印服务器 ····· 43
3.5.1 安装打印机 ····· 44
3.5.2 配置打印机属性 ····· 46
3.5.3 设置打印机权限 ····· 48
3.6 实训 ····· 49
3.7 习题 ····· 50

第 4 章 创建 Active Directory 域 ····· 51

4.1 知识介绍——域和活动目录 ····· 52
4.1.1 活动目录和域的概念 ····· 52
4.1.2 安装域控制器的条件 ····· 54
4.2 任务 1：安装活动目录 ····· 54
4.3 任务 2：将计算机加入域 ····· 60
4.4 任务 3：域用户账户的管理与应用 ····· 61
4.4.1 创建域用户账户 ····· 61
4.4.2 配置域用户账户的属性 ····· 62
4.4.3 利用域用户账户登录 ····· 64
4.5 任务 4：域组的管理与应用 ····· 65
4.5.1 域组的类型及使用范围 ····· 65
4.5.2 域组的创建与管理 ····· 65
4.6 任务 5：管理组织单位 ····· 66
4.6.1 创建和删除组织单位 ····· 67
4.6.2 组织单位的委派 ····· 68
4.7 实训 ····· 70
4.8 习题 ····· 71

第 5 章 本地安全策略与组策略应用 ····· 73

5.1 知识介绍——本地安全策略 ····· 74
5.2 任务 1：设置账户策略 ····· 74
5.2.1 密码策略 ····· 74
5.2.2 账户锁定策略 ····· 75
5.3 任务 2：设置本地策略 ····· 76
5.3.1 审核策略 ····· 77
5.3.2 用户权限分配 ····· 81
5.3.3 安全选项 ····· 82
5.3.4 本地组策略 ····· 83
5.4 知识介绍——组策略 ····· 84
5.4.1 组策略结构 ····· 84
5.4.2 计算机与用户配置 ····· 86
5.5 任务 3：组策略的简单应用 ····· 87
5.5.1 组策略应用实例 ····· 87
5.5.2 组策略应用规则 ····· 90
5.5.3 组策略的筛选 ····· 91
5.6 任务 4：利用组策略实现软件分发 ····· 93
5.7 实训 ····· 96
5.8 习题 ····· 97

第 6 章 磁盘管理 ····· 99

6.1 知识介绍——磁盘管理概述 ····· 100
6.1.1 磁盘类型 ····· 100
6.1.2 磁盘分区 ····· 101
6.2 任务 1：基本磁盘管理 ····· 102
6.2.1 创建主分区 ····· 103
6.2.2 创建扩展分区 ····· 104
6.2.3 创建逻辑分区 ····· 105
6.2.4 删除分区 ····· 105
6.3 任务 2：动态磁盘管理 ····· 106
6.3.1 基本磁盘和动态磁盘的转换 ····· 106
6.3.2 简单卷 ····· 107
6.3.3 跨区卷 ····· 108
6.3.4 带区卷 ····· 109
6.3.5 镜像卷 ····· 110
6.3.6 RAID-5 卷 ····· 111
6.4 任务 3：使用磁盘配额 ····· 112

6.5 实训……114
6.6 习题……114

第 7 章 配置 DHCP 服务……115

7.1 知识介绍——DHCP 概述……116
7.1.1 DHCP 的租约过程……116
7.1.2 更新与释放租约……118
7.2 任务 1：配置 DHCP 服务……119
7.2.1 DHCP 安装要求……119
7.2.2 安装 DHCP 服务……119
7.2.3 授权 DHCP 服务器……121
7.2.4 配置作用域……122
7.2.5 配置服务器选项……128
7.3 任务 2：配置 DHCP 客户机……128
7.4 任务 3：维护 DHCP 服务器……130
7.5 实训……132
7.6 习题……133

第 8 章 配置 DNS 服务……135

8.1 知识介绍——DNS 概述……136
8.1.1 域名空间……136
8.1.2 DNS 查询模式……138
8.2 任务 1：配置 DNS 服务器……140
8.2.1 必要条件……140
8.2.2 安装 DNS 服务器角色……141
8.2.3 新建区域……141
8.2.4 创建资源记录……145
8.3 任务 2：配置 DNS 客户机……147
8.4 任务 3：高级设置……148
8.4.1 转发器……148
8.4.2 DNS 区域传输……150
8.4.3 子域和委派……152
8.4.4 根提示……155
8.5 实训……156
8.6 习题……157

第 9 章 搭建 Web 和 FTP 站点……159

9.1 知识介绍——IIS 与 WWW 服务概述……160
9.2 任务 1：安装和配置 Web 站点……160

9.2.1 安装 IIS ····· 160
9.2.2 配置网站 ····· 162
9.3 任务 2：配置虚拟目录和虚拟主机 ····· 165
9.3.1 配置虚拟目录 ····· 165
9.3.2 配置虚拟主机 ····· 166
9.4 任务 3：保证站点的安全 ····· 170
9.4.1 身份验证和访问控制 ····· 171
9.4.2 IP 地址和域名限制 ····· 173
9.4.3 NTFS 权限 ····· 174
9.4.4 启用日志 ····· 174
9.5 任务 4：安装和配置 FTP 服务 ····· 175
9.5.1 安装 FTP 服务 ····· 175
9.5.2 添加 FTP 站点 ····· 176
9.5.3 FTP 站点的基本设置 ····· 178
9.5.4 配置虚拟目录 ····· 180
9.6 任务 5：使用 FTP 客户端 ····· 181
9.6.1 FTP 命令行 ····· 181
9.6.2 Web 或资源管理器方式 ····· 182
9.7 实训 ····· 182
9.8 习题 ····· 183

第 10 章 远程访问服务（RAS） ····· 185

10.1 知识介绍——远程访问概述 ····· 186
10.2 任务 1：配置远程访问服务 ····· 187
10.2.1 搭建远程访问服务器 ····· 187
10.2.2 激活路由和远程访问服务 ····· 189
10.2.3 配置远程访问服务器 ····· 192
10.2.4 配置客户机网络连接 ····· 196
10.3 任务 2：使用网络策略控制访问 ····· 197
10.3.1 新建网络策略 ····· 198
10.3.2 远程用户访问权限 ····· 203
10.4 实训 ····· 204
10.5 习题 ····· 204

第 11 章 PKI 与证书服务 ····· 205

11.1 知识介绍——PKI 概述 ····· 206
11.1.1 公钥加密技术 ····· 206
11.1.2 PKI 协议 ····· 207
11.2 知识介绍——证书颁发机构 ····· 208

11.2.1 证书 …… 208
11.2.2 CA 的作用 …… 209
11.2.3 CA 的类型 …… 209
11.2.4 证书颁发过程 …… 210
11.3 任务 1：安装证书服务 …… 210
11.4 任务 2：SSL 网站证书应用 …… 215
11.4.1 申请与颁发证书 …… 215
11.4.2 安装与使用证书 …… 219
11.4.3 导入与导出证书 …… 221
11.5 实训 …… 222
11.6 习题 …… 223

第 12 章 远程桌面服务（RDS） …… 225

12.1 知识介绍——远程桌面服务概述 …… 226
12.2 任务 1：部署远程桌面服务 …… 227
12.3 任务 2：部署 RemoteApp …… 231
12.4 实训 …… 234
12.5 习题 …… 235

第 13 章 虚拟化服务 …… 237

13.1 知识介绍——服务器虚拟化概述 …… 238
13.2 任务 1：安装 Hyper-V …… 238
13.3 任务 2：创建虚拟网络 …… 239
13.4 任务 3：创建虚拟机 …… 241
13.5 任务 4：管理虚拟机 …… 244
13.6 实训 …… 246
13.7 习题 …… 246

第 14 章 备份与灾难恢复 …… 247

14.1 知识介绍——Windows 备份工具 …… 248
14.2 任务 1：备份与还原数据 …… 248
14.2.1 备份数据 …… 248
14.2.2 还原数据 …… 252
14.2.3 备份设置 …… 254
14.3 任务 2：Windows 安全模式应用 …… 255
14.4 实训 …… 257
14.5 习题 …… 257

第 1 章

Windows Server 2008 R2 安装

项目需求：

ABC 公司是一家集计算机软／硬件产品营销、技术服务和网络工程于一体的信息技术企业，随着业务拓展和规模的扩大，需要购买 5 台服务器，作为文件服务器、打印服务器、域控制器和网站服务器等，考虑到服务器的硬件条件和能提供的网络服务，新购入的服务器要安装 Windows Server 2008 R2 网络操作系统。

技能目标：

- 理解客户机和服务器的概念
- 了解 Windows Server 2008 版本
- 会安装 Windows Server 2008 R2
- 会初步配置 Windows Server 2008 R2

MEMO

1.1 知识介绍——客户机与服务器

网络一般由计算机、网络连接设备、操作系统以及资源组成。连接设备是连接计算机的各种物理设备，如路由器和交换机等，资源是存储在计算机上的软件、信息和数据，操作系统是管理这些资源的载体。在现存的计算机网络中，主要有以下两种不同的网络管理模式。

1．对等网模式

对等网中主机的地位完全相同，网络中不存在处于管理或者服务核心地位的主机，计算机之间没有客户机和服务器的区别，网络上每一台计算机的地位都是平等的，它们的资源与管理是分散在各个计算机上的，也被称为工作组网络，如图 1-1 所示。对等网只适用于小型家庭网络或者小型企业，计算机数量最多不超过 20 台。

2．客户机／服务器模式

当网络规模扩大，对等网模式不能满足企业发展需要时，应该采用客户机／服务器模式，简称为 C/S 模式，如图 1-2 所示。在这种网络结构中，计算机有了明确的分工，有了客户机与服务器的区别。用户在客户机上向服务器发出服务请求，服务器根据请求的内容来完成相应的工作，将结果传给客户机。

（1）客户机

客户机又称为工作站或客户端，一般是用户使用的计算机。当一台计算机连接到网络上时，就称为局域网中的客户机。客户机是用户和网络的接口设备，用户通过它可以与网络交换信息，共享网络资源。在网络中客户机是一个接入网络的设备，它的接入和离开不会对整个网络产生多大的影响。

（2）服务器

服务器是在网络环境中为客户机提供各种服务的专用计算机，一般用来完成某一特定功能，例如，集中存储网络中信息和数据的文件服务器、发布网站的 Web 服务器、收发电子邮件的邮件服务器等。由于服务器特殊的用途和应用环境，决定了它的硬件配置与普通的 PC 有较大差别。一般服务器采用多处理器、高速内存、大容量 SCSI 接口硬盘，还可能采用磁盘阵列等设备和技术，从而保证系统的可靠性。

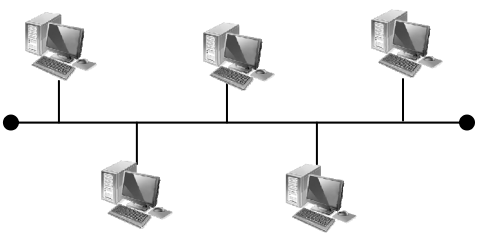


图 1-1　对等网

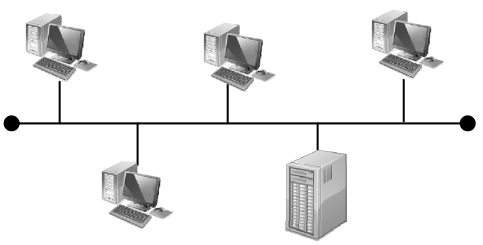


图 1-2　客户机／服务器

1.2　知识介绍——Windows Server 2008 R2 版本

不管是服务器还是客户机，都要基于操作系统才能正常工作。现在主流操作系统包括 Linux 类操作系统、UNIX 类操作系统、Windows 系列操作系统和 MAC 操作系统。Windows 操作系统以其易操作性和人性化的界面受到众多用户的信赖。

Windows 操作系统主要分为两大类，一类面向家庭用户、单机用户和非专业用户，常用作客户机的操作系统主要有 Windows 7、Windows 8、Windows 10 等；另一类主要面向企业用户，称为网络操作系统，不强调对多媒体和娱乐功能的支持，集成了更多的、更完善的网络服务组件，常用作服务器的操作系统主要有 Windows Server 2003、Windows Server 2008、Windows Server 2012、Windows Server 2016。

Windows Server 2008 是 Microsoft 公司在 2008 年 2 月推出的运行在 32 位和 64 位计算机平台上的网络操作系统，在 Windows Server 2003 的基础上增加了一些新的模块和功能。2009 年 10 月又推出只支持 64 位的 Windows Server 2008 R2 版。Windows Server 2008 R2 可以为大、中或小型企业搭建功能强大的网站与应用程序服务器平台，Windows Server 2008 R2 强大的管理功能与经过强化的安全措施，简化了服务器的管理，提高了资源的可用性，有效地保护企业应用程序与数据。Windows Server 2008 R2 家族主要有 7 个版本，每个版本具有不同的网络功能，在实际应用中根据需要选择具体版本。

（1）Windows Server 2008 R2 Foundation Edition（基础版）

该版本是一种成本低廉、容易部署、面向小型企业的操作系统，可以运行最常见的业务应用程序或作为信息分享的平台。

（2）Windows Server 2008 R2 Standard Edition（标准版）

此版本具备主流服务器所拥有的功能，它自带了改进的 Web 和虚拟化功能，这些功能可以提高服务器架构的可靠性和灵活性，同时还能节省时间和成本。利用其中强大的工具，用户可以更好地控制服务器，提高配置和管理任务效率。

（3）Windows Server 2008 R2 Enterprise Edition（企业版）

此版本提供了更高的可用性和扩展性，是高级服务器平台。在虚拟化、节电以及管理方面增加了新功能，使得移动办公的员工可以更方便地访问公司的资源。

（4）Windows Server 2008 R2 Datacent Edition（数据中心版）

此版本是一个专门在小型和大型服务器上部署关键业务应用和大型虚拟化设计的企业级平台，除了提供企业版相同功能，还支持 2～64 个处理器，并且可以构建企业级虚拟化解决方案。

（5）Windows Web Server 2008 R2（Web 版）

此版本是特别为 Web 服务器而设计的，它拥有多功能的 IIS7.5，是一个专门面向 Internet 应用而设计的服务器操作系统，它改进了管理和诊断工具，可以在各种常用开发平台中使用。

（6）Windows Server 2008 R2 for Itanium-Based Systems（安腾版）

此版本是一个企业级的平台，可以用于部署关键业务的应用程序，为高度动态化的 IT 架构提供基础。

（7）Windows HPC Server 2008 R2 （高性能版）

此版本是下一代高性能计算（High-Performance Computing）平台，为高效率的 HPC 环境提供了企业级的工具。该版本能有效利用上千个处理器核心，并通过管理控制台监控及维护系统健康状态和稳定性。

1.3 任务 1：安装 Windows Server 2008 R2

ABC 公司购买的 5 台服务器要安装 Windows Server 2008 R2 企业版操作系统，首先需要检查一下服务器硬件条件能否满足 Windows Server 2008 R2 企业版最低硬件配置要求，选择安装类型。

1.3.1 硬件配置及安装类型

Windows Server 2008 R2 企业版对计算机硬件兼容性要求较高，如表 1-1 所示。

表 1-1 Windows Server 2008 R2 企业版的硬件要求

硬　件	要求（最低）	推　荐
处理器（CPU）	1.4 GHz	＞2 GHz
内存（RAM）	512 MB	＞2 GB
硬盘	32 GB	＞40 GB
显示器	VGA（800×600）	
其他	DVD 光驱、键盘、鼠标	

在安装 Windows Server 2008 R2 时，需要考虑采用全新安装还是升级安装。此外，还要根据对服务器的安全、性能要求，决定进行完全安装还是服务器核心安装。

1．全新安装和升级安装

全新安装是最常见的安装方式，当计算机上没有安装 Windows Server 2008 R2 之前的版本时，适合采用全新完全安装；当计算机已安装了 Windows Server 2008 R2 之前的版本时，可以在不破坏以前各种设置的前提下升级系统。

2．完全安装和服务器核心安装

完全安装是传统的安装模式，同时安装图形用户界面和命令提示行界面，能充当各种服务器角色。服务器核心安装类似“精简版”安装，仅提供最小化环境，减小了对硬件资源的消耗和受攻击面，但只能使用命令管理系统，仅支持部分服务器角色。

1.3.2　安装步骤

STEP1 首先将 Windows Server 2008 R2 的安装光盘放入光驱，然后在 BIOS 中修改计算机启动顺序为 CD-ROM。开机后，计算机首先查看 CD-ROM 中是否有可以直接引导计算机启动的光盘，如果找到启动文件，直接进入 Windows Server 2008 R2 安装程序的输入语言和其他选项，如图 1-3 所示。

图 1-3　语言和其他选项

STEP2 单击“下一步”按钮，在如图 1-4 所示的对话框中单击“现在安装”按钮。

图 1-4　安装 Windows

STEP3 在如图 1-5 所示的对话框中选择要安装的版本，单击“下一步”按钮。

图 1-5　选择 Windows 版本

STEP4 阅读许可条款，选择“我接受许可条款”，单击“下一步”按钮，如图 1-6 所示。

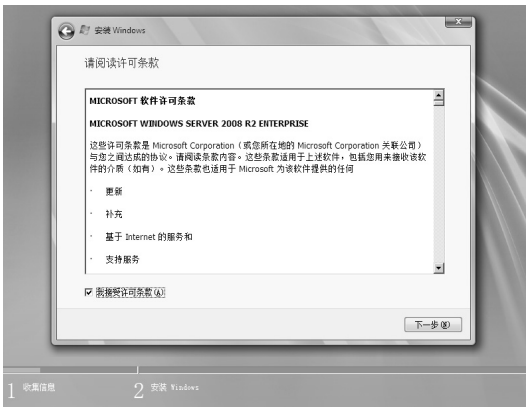


图 1-6　阅读许可条款

STEP5 在如图 1-7 所示对话框中选择安装类型，这里选择“自定义（高级）”项。

图 1-7　选择安装类型

STEP6 选择安装位置，在如图 1-8 所示对话框中选择将要安装 Windows 的磁盘分区，单击“下一步”按钮。

图 1-8　选择安装位置

STEP7 系统开始安装并提示安装程序已经运行到哪个步骤，如图 1-9 所示。

图 1-9　正在安装 Windows

STEP8 安装完成后系统将自动重新启动，第一次启动 Windows Server 2008 R2 时会自动以系统管理员账户 Administrator 登录系统。用户首次登录时必须更改 Administrator 密码，单击“确定”按钮，输入新密码与确认密码后单击向右的箭头图标，如图 1-10 所示。

服务器核心安装与完全安装步骤基本一致，只需要在图 1-5 中选择“服务器核心安装”，密码设置完成登录后只有命令行工具，需要输入命令来操控计算机。如图 1-11 所示。

图 1-10　设置 Administrator 密码

图 1-11　服务器核心版登录界面

注意:

系统默认用户的密码必须至少 6 个字符，并且不可包含用户账户名称中超过两个以上的连续字符，至少包含字母、数字和非数字 3 种字符。

1.4　任务 2：Windows Server 2008 R2 基本配置

当 Windows Server 2008 R2 安装完成后，需要添加相应的角色或功能，才能使其完成服务功能。

1.4.1 初始配置

系统成功登录后会出现初始配置任务窗口，帮助管理员完成服务器的安装和初始化配置，诸如更改计算机名称、更改用户账户、启用远程桌面和更改防火墙状态等。表 1-2 显示了 Windows Server 2008 R2 初始化配置的默认设置。该窗口的“添加角色”和“添加功能”命令可以向服务器添加角色和功能，初始配置任务如图 1-12 所示。

表 1-2 Windows Server 2008 R2 初始化配置的默认设置

设 置 项	默 认 配 置
计算机名称	在安装过程中随机分配
域成员身份	默认情况下未加入域，而是加入一个名为 WORKGROUP 的工作组
Windows 自动更新	Windows 自动更新默认为关闭状态
网络连接	所有的网络连接设置为使用 DHCP 自动获取 IP 地址
Windows 防火墙	Windows 防火墙默认为打开状态
已安装角色	默认情况下未安装任何角色

图 1-12 初始配置任务

1.4.2 添加角色

服务器角色是软件程序的集合，在安装并正确配置后，计算机将为网络内的用户或其他计算机执行特定功能。下面以安装文件服务角色为例说明添加角色的步骤。

STEP1 选择“开始”→“管理工具”，打开“服务器管理器”页面，在“角色”中单击“添加角色”按钮，在“选择服务器角色”页面中选择“文件服务”，如图 1-13 所示，单击“下一步”按钮。

STEP2 在文件服务器简介页面中，说明了提供的服务以及注意事项，单击“下一步”按钮，出现“选择角色服务”页面，选择为文件服务安装的角色服务，单击“下一步”按钮，如图 1-14 所示。

图 1-13　添加服务器角色

图 1-14　选择角色服务

STEP3 确认后进入“安装进度”页面，显示正在安装，当安装完成后，显示安装成功，关闭安装窗口。

1.4.3　添加功能

功能是一些软件程序，这些程序不直接构成角色，但可以支持或增强一个或多个角色的功能。如在客户端通过 Telnet 与服务器进行远程通信，需要在服务器上安装 Telnet 服务器功能。

添加功能的方法与添加角色的方法相似，在“服务器管理器”页面中选择“功能”，单击“添加功能”按钮，在“选择功能”页面选择“Telnet 服务器”，如图 1-15 所示，单击“下一步”按钮，按照提示完成功能添加。

图 1-15　选择功能

1.5　实训

实训环境

HT 公司作为一家大型系统集成服务提供商，经营网络项目集成业务，包括网络集成、解决方案、代理产品和技术服务等。公司最近购置了一批服务器作为文件、打印服务器，网络管理员需要为这些服务器安装 Windows Server 2008 R2 操作系统。

需求描述

- 使用 Windows Server 2008 R2 安装光盘安装操作系统。
- 查看“系统属性”。
- 查看硬件信息。
- 添加文件服务角色。
- 添加远程协助功能。

1.6　习题

- 常见的网络管理模式有几种？各自具有什么特点？
- 服务器与普通 PC 有哪些区别？
- Windows Server 2008 R2 有哪些版本？
- Windows Server 2008 R2 系统完全安装与服务器核心安装有哪些区别？

第 2 章

配置网络与工作组环境

项目需求：

ABC 公司的 5 台服务器安装了 Windows Server 2008 R2 操作系统后，进行了简单配置。接下来的任务是使服务器之间网络连通，并具有代表各自用途的计算机名。考虑到有的服务器供多人使用，还要按部门为使用服务器的员工创建用户账户和组，并对用户进行密码修改、组的归属等管理。

技能目标：

- 理解 IP 地址和计算机名的概念
- 会配置计算机的 IP 地址
- 会使用 Windows 网络测试工具
- 理解工作组的特点
- 会管理本地用户账户
- 会管理本地组账户

MEMO

2.1 知识介绍——Windows 网络组件与 IP 地址

2.1.1 Windows 网络组件

要将安装 Windows Server 2008 R2 操作系统的计算机接入网络，需要具有网络适配器和网络协议，并配置好相应的 IP 地址等网络参数。

1．网络适配器

网络适配器又称网卡，是常用的网络硬件设备。计算机通过网络适配器连接到网络电缆、光缆或其他网络介质。通常情况下，网络适配器按速率分为 10 Mb/s、100 Mb/s、1 000 Mb/s 以及自适应网卡等，按使用介质分为双绞线网卡、光纤网卡和无线网卡等。在局域网中使用较多的是 100 Mb/s 和 1 000 Mb/s 自适应网卡，通过设备管理器可以查看当前的网卡。

2．协议

协议是计算机与网络设备之间，计算机与计算机之间的通信语言，只有两者之间使用了相同的协议才能够通信和访问。TCP/IP 协议是目前最完整、最常用的网络通信协议，它可以使不同网络架构、不同操作系统的计算机之间相互通信。Windows Server 2008 R2 操作系统默认安装 TCP/IP 通信协议，支持 IPv4 和 IPv6 两种网络协议。

2.1.2 网络参数

互联网上连接了无数的网络设备和计算机，每一台主机都有唯一的地址，作为该主机在 Internet 上的唯一标识，即 IP 地址，目前有 IPv4 和 IPv6 两个版本，当前广泛应用的是 IPv4。

1．IP 地址的格式

IP 地址由 32 位二进制数组成，而且在 Internet 范围内是唯一的。例如，连接在 Internet 上的一台计算机的 IP 地址如下所示。

```
00111101. 10100111. 10011100. 01101100
```

很显然，这些数字不容易记忆且可读性比较差，因此，人们将组成计算机 IP 地址的 32 位二进制分成四段，每段八位，中间用圆点隔开，然后将每八位二进制数转换为十进制，这样上述二进制格式的 IP 地址就变成了 61.167.156.108。

注意：

IPv6 是下一代 IP 协议，由 128 位二进制组成，分为 8 段，以冒号隔开。Windows Server 2008 R2 也支持 IPv6，目前尚没有普遍使用。本书中的 IP 地址均采用 IPv4 版本。

2．IP 地址的分类

IP 地址由网络部分（netID）与主机部分（hostID）两部分组成。网络部分用于标识不同的网络，主机部分用于标识一个网络中的特定主机。IP 地址的网络部分由 IANA（Internet 地址分配机构）统一分配，以保证 IP 地址的唯一性。

为了便于分配和管理，IANA 将 IP 地址分为 A、B、C、D、E 五类，其中 A、B、C 三类 IP 地址可供一般主机使用，网络 ID 与主机 ID 划分有相应的规则。D、E 两类不划分网络 ID 与主机 ID，D 类地址是用于组播通信的地址，E 类地址是用于科学研究的保留地址，它们不能在互联网上作为节点地址使用。

A 类 IP 地址规定第一个 8 位组为网络部分，其余三个 8 位组为主机部分，即 A 类地址=网络+主机+主机+主机。由于 A 类地址网络号为 0 的第一个地址块和网络号为 127 的最后一个地址块保留为特殊用途，A 类地址的有效取值范围为 1～126，可以提供 126 个 A 类网络。每个 A 类网络可以拥有最大主机数目为 2^{24}–2=16 777 214 个（减 2 是去掉主机部分全为 0 和全为 1 的两个地址）。由此可见，A 类 IP 地址适合于大型网络。

注意：

127.0.0.1 又称为本地回环地址，通常用于在本机上 ping 此地址来检查 TCP/IP 协议安装是否正确。除了 127.255.255.255.255，凡是以 127 开头的 IP 地址都代表本机。

B 类 IP 地址规定前两个 8 位组为网络部分，后两个 8 位组为主机部分，即 B 类地址=网络+网络+主机+主机。每个 B 类地址拥有的最大主机数为 2^{16}–2=65 534 个。由此可见，B 类 IP 地址适合于中等规模的网络。

C 类 IP 地址规定前三个 8 位组为网络部分，最后一个 8 位组为主机部分，即 C 类地址=网络+网络+网络+主机。第一个 8 位组取值范围为 192～223，每个 C 类地址拥有最大主机数为 2^{8}–2=254 个。由此可见，C 类 IP 地址适合于小型网络。

目前，在 Internet 上只使用 A、B、C 三类地址，为了满足企业用户在 Intranet（内联网）上使用需求，从 A、B、C 三类地址中分别划出一部分地址供企业内部网络使用，这部分地址称为私有地址。私有地址不能在 Internet 上使用，包括以下 3 组：

- 10.0.0.0～10.255.255.255；
- 172.16.0.0～172.31.255.255；
- 192.168.0.0～192.168.255.255。

3．子网掩码

在网络中不同主机之间的通信有两种情况，一种是同一个网段中两台主机之间相互通信，另一种是不同网段中两台主机之间相互通信。具有相同网络地址的 IP 地址称为同一个网段的 IP 地址。

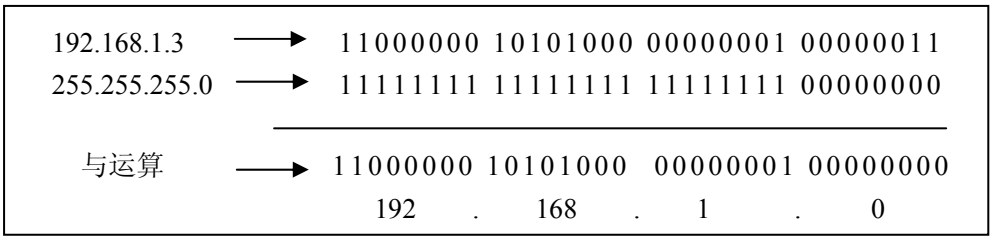
如果同一网段内两台主机通信，则主机将数据直接发送给另一台主机；如果不在同一个网段内的两台主机通信，则主机将数据送给网关，再由网关转发。为了区分这两种情况，进行通信的计算机需要获取远程主机 IP 地址的网络部分以做出判断。如果源主机的网络地址等于目标主机的网络地址，则为同一个网段主机间通信；如果源主机的网络地址不等于目标主机的网络地址，则为不同网段主机间通信。因此，相互通信的计算机首先要获取对方 IP 地址

的网络地址信息，这就需要借助子网掩码。

子网掩码与 IP 地址一样，也是由 32 位二进制数组成的，对应 IP 地址的网络部分用 1 表示，对应 IP 地址的主机部分用 0 表示，通常也用 4 个点分十进制数表示。当为网络中的主机分配 IP 地址时，也要一并给出主机所使用的子网掩码。

- A 类地址的默认子网掩码是 255.0.0.0；
- B 类地址的默认子网掩码是 255.255.0.0；
- C 类地址的默认子网掩码是 255.255.255.0。

有了子网掩码后，只要把地址和子网掩码进行逻辑“与”运算，所得的结果就是 IP 地址的网络地址。例如，给出 IP 地址 192.168.1.3，子网掩码 255.255.255.0，将 IP 地址和子网掩码进行“与”运算，可得出 IP 地址的网络 ID。



使用点分十进制的形式表示掩码书写比较麻烦，为了书写简便，可以使用“IP 地址 / 掩码中 1 的位数”来表示，如 192.168.1.100/24。

4．DNS

在 IP 网络诞生的前十年，人们不得不像记忆电话号码一样记忆主机的 IP 地址，直到 1983 年 DNS（Domain Name System）诞生。在 DNS 服务器中，可以为每台待访问的计算机分配一个名称，如“www.taobao.com”，将这些名称和主机的 IP 地址对应存储在 DNS 服务器上，人们只需要记住主机名称，访问时本地主机通过 DNS 服务器查询到目标主机的 IP 地址。由于主机名称存储在 DNS 服务器中，而非每台计算机中，所以需要为计算机分配的参数是 DNS 服务器的 IP 地址，通常设置首选 DNS 服务器和备用 DNS 服务器，以保证本地计算机查询的成功率。

5．配置 IP 地址

为计算机设置 IP 地址的方法有两种，一种是自动获取，一种是手动配置。

自动获取 IP 地址是 Windows Server 2008 R2 的默认方式，计算机会自动向网络中的 DHCP 服务器租用 IP 地址，如果找不到 DHCP 服务器，则会用 Automatic Private IP Addressing 机制自动为自己设置一个符合 169.254.0.0/16 格式的 IP 地址。自动获取方式可以减轻系统管理员手动设置的负担，并可以避免手工设置可能发生的错误，当网络中计算机数量较多的时候通常采用此方式。

手动配置 IP 地址的计算机接入网络不容易受环境影响而发生变动，也没有自动获取产生的延迟，更节省了自动获取带来的网络开销，但会增加系统管理员的负担。为计算机配置 IP 地址的步骤如下。

STEP1 在桌面上右键单击“网络”图标，选择“属性”，在出现的对话框中“查看活动网

络”部分单击“本地连接”，如图 2-1 所示。

STEP2 在如图 2-2 所示的对话框中单击“属性”按钮。

图 2-1　网络属性

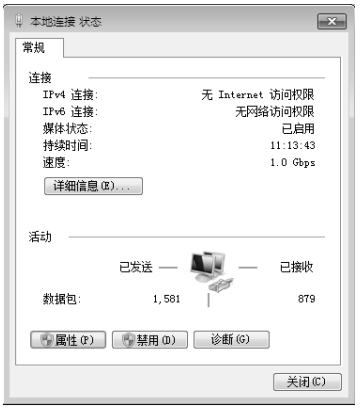


图 2-2　本地连接属性

STEP3 在如图 2-3 所示的对话框中选择“Internet 协议版本 4（TCP/IPv4）”，单击“属性”按钮。在出现的对话框中选择“使用下面的 IP 地址”，设置 IP 地址和子网掩码、默认网关等参数，如图 2-4 所示。

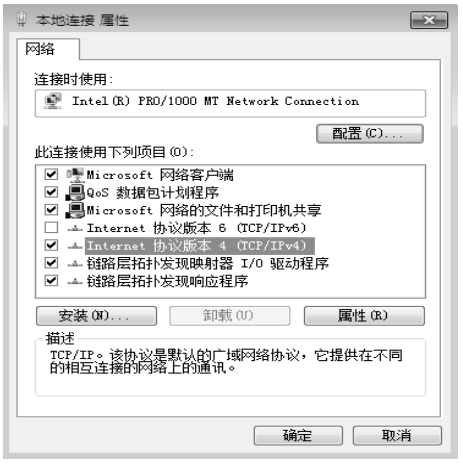


图 2-3　本地连接属性

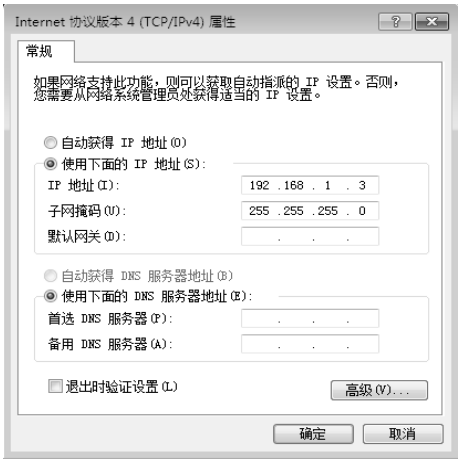


图 2-4　静态 IP 地址

2.2　知识介绍——网络测试工具与计算机名称

2.2.1　网络测试工具

Windows 提供了大量的命令用来测试网络的连通性，下面列举介绍一些常用命令行方式下的网络测试工具。

1．ipconfig

在配置了 IP 地址之后，使用 ipconfig 命令可以检查 IP 配置是否生效。ipconfig 用于查看计算机 IP 地址配置信息，包括 IP 地址、子网掩码和默认网关。使用 ipconfig/all 命令可以查看详细的 IP 地址信息，包括主机名、网卡类型和名称、网卡物理地址和 DNS 服务器等信息。ipconfig/all 命令执行后的显示结果如图 2-5 所示。

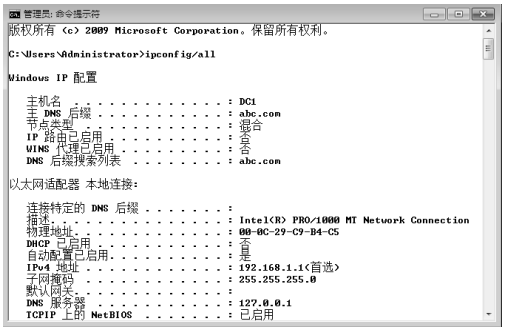


图 2-5　ipconfig/all 命令执行后的显示结果

2．ping

Ping 命令是验证特定 IP 地址是否可以访问的工具，用于测试网络是否连通，使用格式为“ping 目的 IP 地址”，如 ping 192.168.1.100。如果出现如图 2-6 所示的结果，则表明源计算机与目标计算机 192.168.1.100 连通；如果出现如图 2-7 所示的结果，则表明源计算机与目标计算机不连通。

ping 的原理是向目的地发送 4 次数据包，如果收到对方反馈的信息则代表网络通；如果在指定的时间内没有收到，则视为超时，在某些情况下则代表网络不通。如果没有设置网关参数而 ping 一个其他网段的地址，就会出现图 2-8 所示的结果。

图 2-6　ping 命令测试网络连通

图 2-7　ping 命令测试网络不连通

注意：

如果目标主机启用了防火墙的相关设置，ping 命令所发送的数据包可能会被防火墙阻止，即使网络配置正常可能也会显示如图 2-9 所示的结果。如果 ping 的目标主机不存在，也会出现图 2-7 所示的结果。

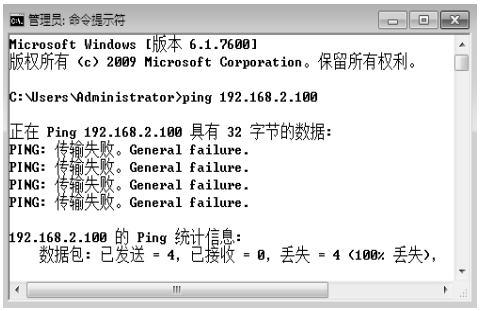


图 2-8　未设置网关，ping 命令测试网络不连通

图 2-9　启用防火墙设置，ping 命令测试网络不连通

结合 ping 命令的参数能实现更高级的功能，如使用“–t”参数指定在中断前执行 ping 命令，可以向目的地持续发送回显请求信息；要中断并显示统计信息，按“Ctrl+Break”组合键；要中断并退出 ping 操作，按“Ctrl+C”组合键。

ping 命令帮助验证 IP 级别的连接，在排除故障时，可以使用 ping 命令向目标主机名或 IP 地址发送 ICMP 回显请求。一般情况下可以按照下列顺序诊断网络连接。

- ping 127.0.0.1，以验证本地计算机上是否正确地配置了 TCP/IP。
- ping 本地计算机的 IP 地址，以验证其是否已正确添加到网络中。
- ping 默认网关的 IP 地址，以验证默认网关是否正常工作以及是否可以与本地网络上的主机进行通信。
- ping 远程主机的 IP 地址，以验证是否可以通过路由器进行通信。

2.2.2　计算机名称与工作组

1．计算机名称

计算机名称用来标识计算机在网络中的身份，就如同人的名字。在同一网络中计算机名字是唯一的，当启动计算机时，系统会在网络上注册唯一的计算机名称，就是从网络中看到的计算机名。要查看本机的计算机名，可以用 nbtstat－n 命令，还可以在桌面上右键单击“计算机”图标，选择“属性”，在如图 2-10 所示的页面中查看计算机名。

在如图 2-10 所示的页面中单击“更改设置”，会出现如图 2-11 所示的“系统属性”页面，单击“更改”按钮，可以更改计算机名与工作组名，如图 2-12 所示。更改后按照提示重新启动计算机后，这些更改才会生效。

注意:

计算机名称使用的标准字符是从 0～9 的数字、从 A～Z 的大写和小写字母以及连字符“-”，但计算机名称不能全部是数字。客户端计算机命名可以按照使用者的姓名或者使用者的岗位命名，服务器的命名一般以服务器的功能命名。

图 2-10　查看计算机名

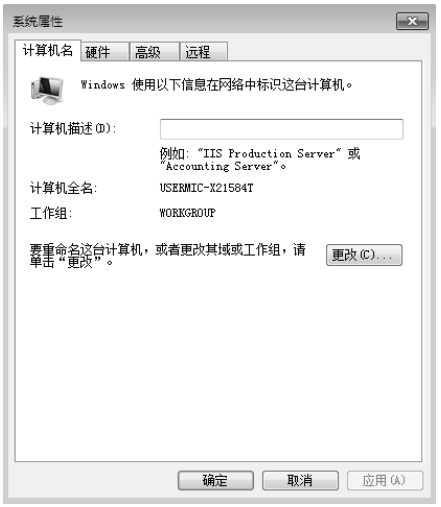


图 2-11 “计算机名”选项卡

图 2-12 “计算机名 / 域更改”对话框

2．工作组

在小型办公网络中，可能有多台计算机。这些计算机地位是平等的，它们组成一个工作组。工作组是一种简单的计算机分组模型，通常用于家庭和小规模网络。工作组中的计算机直接相互通信，不需要服务器来管理网络资源。具有以下特点：

- 每一台计算机都独立维护自己的资源，不集中管理所有的网络资源。
- 每一台计算机都在本地存储用户账户。
- 一个账户只能登录到一台计算机。
- 工作组中的计算机的地位是平等的，对于其他计算机来说既是服务器，也是客户机。
- 工作组的网络规模较小。

一般情况下，可以按照不同的地理位置或部门将计算机加入不同的工作组。查看修改计算机所属工作组与查看修改计算机名称的方法相同。

注意：

工作组名不能和计算机名相同，必须以管理员或 Administrator 组成员身份登录才能完成修改工作组和计算机名的操作。

2.3　任务 1：创建与管理本地用户账户

当计算机启动后，用户必须使用合法的用户名和正确的密码才能进入系统。用户就是计算机使用者在计算机系统中的身份映射，不同身份拥有不同权限。本地用户账户存储在本地的 SAM 数据库里，SAM 文件存放在%systemroot%\ system32\config 文件夹下，其中存放了本地计算机内的组账户和用户账户信息，每个用户账户有唯一的安全标识符 SID（Security IDentifier），用户的权限是通过用户的 SID 记录的。

系统安装完成后会自动创建内置用户账户，它们具有特殊用途，一般不需要更改。Administrator 是默认的管理员账户，其权限最高，在没有其他管理员账户的情况下，建议不要将该账户禁用；Guest 账户是用于临时访问的账户，默认权限很少，且默认状态是禁用的，不建议启用。

注意：

本地账户只能登录到本计算机，主要用于工作组环境中。系统默认只有 Administrator 组内的用户才有权限管理用户与组账户，新创建的用户只具有很少的权限。在“注册表编辑器”窗口中可以查看用户 SID，展开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList 项，其中的子项名称就是用户 SID。

2.3.1　创建本地用户账户

选择“开始”→“管理工具”→“计算机管理”，在如图 2-13 所示的“计算机管理”窗口单击“本地用户和组”，右键单击“用户”，选择“新用户”。在出现的对话框中输入用户名、描述和密码等信息，单击“创建”按钮，如图 2-14 所示。

图 2-13　“计算机管理”窗口

图 2-14　创建用户

在创建用户时，在如图 2-14 所示的对话框中需要输入以下信息。

- 用户名：用户登录时所使用的名字，不能与当前系统中其他用户账户或组账户同名。用户名最长 20 个字符，不区分大小写，也可以使用中文，但不能使用特殊字符（“/、[]：；=*+？<>）。
- 全名和描述：用户的完整名称，用来描述用户个人信息的说明文字，为可选项。
- 密码和确认密码：输入用户将来登录时所使用的密码，输入两次而且必须相同。密码的最大长度是 127 位。系统默认用户的密码必须至少 6 个字符，至少包含 A～Z、a～z、0～9 和非字母数字等 4 组字符中的 3 种，并且字母区分大小写。
- 用户下次登录时须更改密码：用户在下次登录时，系统会显示一个要求用户更改密码的对话框，这个操作可以确保只有该用户知道自己的密码。
- 用户不能更改密码：默认情况下，每个用户都可以更改自己的密码，当多个用户使用同一个账户时，其中一个人更改了密码会造成其他用户不能登录。禁止用户更改密码可以避免这种情况。
- 密码永不过期：系统默认 42 天后密码会过期，选择此项后密码将永不过期。
- 账户已禁用：若某用户暂时离开不需要登录系统，可以将账户禁用，禁用后此账户将不能登录。

用户创建完成后，注销当前登录的用户，在如图 2-15 所示的登录界面单击新建的用户登录。

图 2-15　新用户登录

2.3.2　设置账户属性

当用户账户建立完成后，还可以设置账户的一些属性。右键单击用户名，选择“属性”，显示用户属性对话框，其中有多个选项卡，如图 2-16 所示。用户账户的属性包括以下几个部分。

- 常规：“常规”选项卡可以修改用户的基本信息，如图 2-16 所示。
- 隶属于：“隶属于”是指用户账户所属的组，通过“隶属于”选项卡可以将用户添加到组中，也可以将用户从组中删除。通过这个选项卡可以大致判断用户的权限，如果用户隶属于管理员组，则用户具有管理员权限，如图 2-17 所示。
- 配置文件：配置文件用于保存用户工作时使用的环境信息，如桌面、我的文档和收

藏夹等。在配置文件选项卡中可以修改配置文件的存储路径。

图 2-16　“常规”选项卡

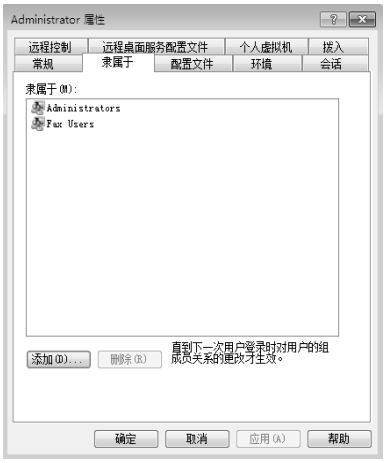


图 2-17　“隶属于”选项卡

2.3.3　修改和删除用户账户

1. 修改账户密码

修改账户密码有两种情况，一种是管理员为用户修改密码，管理员不需要知道用户的密码即可修改；另一种是用户自行修改密码，用户必须知道该账户的原始密码才能修改。

用管理员账户登录系统后，在如图 2-18 所示的页面中右键单击要修改密码的账户，选择“设置密码”项，出现警告信息，单击“继续”按钮，输入两次新密码并确定，完成密码修改。

图 2-18　设置用户密码

用户在为自己的账户修改密码时，登录系统后按“Ctrl+Alt+Delete”组合键，出现如图 2-19 所示的“Windows 安全”页面，单击“更改密码”按钮，按照提示输入原来的旧密码，再输入两次新密码完成修改。

图 2-19 “Windows 安全”页面

2．重命名用户账户

当一个员工离职，另一个员工接替工作时，可以将以前员工使用的用户账户更改为新员工的账户，并重设密码。更名后原用户账户所有权限将全部保留下来。在如图 2-18 所示的“计算机管理”窗口右键单击要重命名的账户，选择“重命名”项，该用户的名字变成可编辑状态，输入新用户名后，按回车键或单击空白处，完成修改。

3．删除用户账户

当用户账户确定不需要使用时，可以删除。当一个用户被删除后，再建立同名用户账户，不能保留以前的权限。原因是在系统内部有唯一标识用户的 SID，新建立的同名用户 SID 与被删除的原用户不同。右键单击要删除的账户，选择“删除”项可完成删除操作。

2.4 任务 2：创建与管理本地组

当需要为多个用户设置相同权限时，逐一设置比较烦琐，可以使用组来简化操作。组是账户的集合，合理使用组来管理用户账户权限，能够为管理员减轻负担。例如，当针对业务部设置权限后，业务部内的所有用户都会自动拥有此权限，不需要单独为每个用户设置权限。

与用户账户相似，安装完操作系统后会自动建立一些特殊用途的内置组，常用内置本地组简要说明见表 2-1。用户还可以创建本地组，在如图 2-13 所示的“计算机管理”页面中，右键单击“组”，选择“新建组”选项，出现如图 2-20 所示的“新建组”对话框，按照要求输入组名，单击“添加”按钮为该组添加用户，单击“创建”按钮，完成组的创建。

表 2-1 常用内置本地组简要说明

组名	描 述 信 息
Administrators	该组的成员具备管理员权限，默认的管理员账户 Administrator 属于该组
Guests	该组的成员拥有一个在登录时创建的临时用户配置文件，注销时配置文件被删除，默认的 Guest 账户属于该组

续表

组名	描 述 信 息
Users	该组是新用户的默认组，拥有一些基本权限，如运行应用程序、使用本地和网络打印机、锁定计算机等，但不能共享文件，不能关闭计算机
INTERACTIVE	这类内置组成员是由 Windows 程序自动添加的，INTERACTIVE 动态包含在本地登录的所有用户
Authenticated Users	这类内置组成员也是由 Windows 程序自动添加的，组中动态包含通过验证的所有用户
Everyone	这类内置组成员也是由 Windows 程序自动添加的，该组包含任何用户（包括 Guest 用户），设置开放权限时经常使用

图 2-20　创建本地组

如果要进行为组重命名、删除组和为组添加用户等操作，可以右键单击组名，在弹出的快捷菜单中完成各项操作。

2.5　实训

实训环境

HT 公司有多台 Windows Server 2008 R2 服务器需要互连，这些服务器位于 192.168.10.0/24 和 10.0.0.0/8 网段，网络管理员需要为这些服务器配置网络组件，使其连通。其中一台名叫 Filesvr 的服务器被临时配置为文件服务器，业务部的员工想从自己的计算机访问服务器上的共享文件夹 share。

需求描述

- 规划计算机名称和 IP 地址。
- 为计算机配置 IP 地址、子网掩码和默认网关。
- 使用 Windows 测试工具调试网络。
- 创建本地用户账户 user1、user2 和 user3，创建本地组“业务部”。
- 将用户账户加入到组中。
- 分别使用 user1、user2 和 user3 账户通过网络访问共享文件夹 share。

2.6 习题

- 在什么情况下适合采用工作组模式？工作组有哪些特点？
- 分别说明 ipconfig 和 ping 命令的作用。
- 查找资料，了解系统默认的组有哪些，具有哪些功能？
- 本地用户账户文件存储在哪里，文件名是什么？

第 3 章

文件和打印服务器

项目需求：

ABC 公司的一台公共服务器上放置了各部门的资料，为保障数据的安全，需要限制不同用户访问该计算机资源时的访问权限，如部门经理可以写入数据，普通用户可以读取数据；公司某员工离职后，他使用过的计算机上有重要文件管理员无法查看，要重新设置 NTFS 访问权限取得文件的所有权，重新设置访问权限；此服务器上还连接着一台打印设备，希望该服务器为全体员工提供打印服务，而且经理较普通员工有优先打印权限。

技能目标：

- 理解 NTFS 权限的概念
- 会管理 NTFS 权限
- 理解复制和移动对权限的影响
- 会创建和访问共享文件
- 理解共享权限和 NTFS 权限的关系
- 理解打印设备和打印机的区别
- 会配置打印池和打印机优先级
- 会配置打印权限

MEMO

3.1 知识介绍——NTFS 权限

3.1.1 NTFS 权限概述

文件在磁盘上的存储格式又叫文件系统，Windows 常见的文件系统有 FAT 和 NTFS。NTFS（New Technology File System）是微软公司随着 Windows NT 推出的文件系统，同 FAT 相比，NTFS 在磁盘读写性能、可靠性、安全性、磁盘空间利用率方面有很大改善，Windows 的部分功能必须在 NTFS 文件系统上才能实现，如活动目录。NTFS 文件系统主要特性如下。

- 访问控制列表（Access Control List，ACL）：可以限定用户或组对文件或文件夹的访问权限。
- 加密文件系统（Encrypting File System，EFS）：加密文件内容，保障数据安全。
- 压缩文件、文件夹，以节省磁盘空间。
- 支持磁盘配额：可以限定每个用户使用的最大磁盘空间，保障同一磁盘分区能够为多用户使用。

NTFS 文件系统可以针对不同用户或组设置多个访问权限，这些访问权限可以提供文件的安全性。在 NTFS 文件系统中，每个文件或文件夹的属性中都增加了一个“安全”选项卡，其中包含访问控制列表和访问控制项。访问控制列表中列出的是和当前文件或文件夹权限有关的用户和组，当选中某个用户或组后，访问控制项中列出的是和该用户或组相关的权限，如图 3-1 所示。

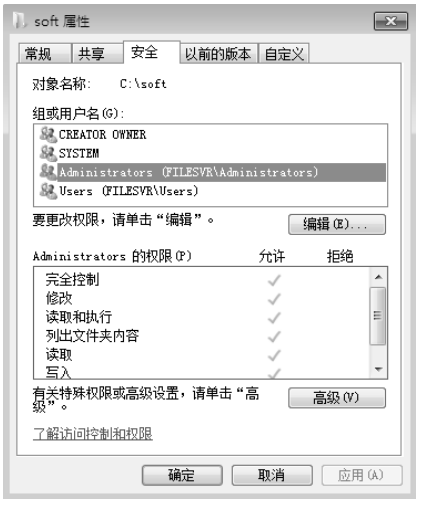


图 3-1 文件夹“安全”选项卡

当一个用户试图访问一个文件或者文件夹时，NTFS 文件系统会检查访问控制列表中是否存在该用户账户或该用户所在的组，然后再进一步检查访问控制项，根据控制项中的权限来判断用户最终权限。如果访问控制列表中不存在该用户账户或其所在的组，则拒绝该用户访问。

3.1.2　文件和文件夹权限

用户对 NTFS 磁盘内的文件或数据拥有适当权限后，才能访问这些资源。权限可以分为标准权限与特殊权限，标准权限可以满足一般需求，特殊权限可以更精确地分配权限。

标准的 NTFS 文件权限如下所述。

- 读取：可以读取文件内容，查看文件属性与权限。
- 写入：可以修改文件内容、向文件中添加数据或修改文件属性等。
- 读取和执行：除了拥有读取的所有权限，还具备运行应用程序的权限。
- 修改：除了拥有读取、写入、读取和执行的所有权限，还可以删除文件。
- 完全控制：不仅拥有所有的 NTFS 文件权限，即上述所有权限，而且还拥有更改权限与取得所有权的特殊权限。

标准的 NTFS 文件夹权限如下所述。

- 读取：可以查看文件夹内的文件与子文件夹名，查看文件夹属性与权限等。
- 写入：可以在文件夹内新建文件与子文件夹，修改文件夹属性等。
- 列出文件夹内容：除了拥有读取的所有权限，还具备遍历文件夹的权限，即打开或关闭此文件夹。
- 读取和执行：拥有与列出文件夹内容几乎完全相同的权限，只有在权限继承方面有所不同。列出文件夹内容权限只会被文件夹继承，而读取和执行会同时被文件夹与文件继承。
- 修改：除了拥有上述所有权限，还可以删除文件夹。
- 完全控制：拥有所有的 NTFS 文件夹权限，以及更改权限与取得所有权的特殊权限。

注意：

只有 Administrator 组内的成员、文件及文件夹的所有者和具有完全控制权限的用户，才有权限设置 NTFS 权限。

3.2　任务 1：应用 NTFS 权限

3.2.1　简单应用

ABC 公司的一台文件服务器名为 Filesvr，服务器上有一个名为 tools 文件夹，根据工作需要，用户 userA 需要读取 tools 文件夹的内容，但不能修改文件夹内容，用户 userB 需要读取和修改 tools 文件夹的内容。

STEP1　右键单击 tools 文件夹，选择“属性”，在“tools 属性”对话框中选择“安全”选项卡，在如图 3-2 所示的对话框单击“编辑”按钮，出现“tools 的权限”对话框，单击“添加”按钮，输入用户账户名 userA，如图 3-3 所示，单击“确定”按钮。还可以单击图 3-3 中的“高级”按钮，在出现的对话框中单击“立即查找”，从列表中选择用户或组，推荐使用此方法。

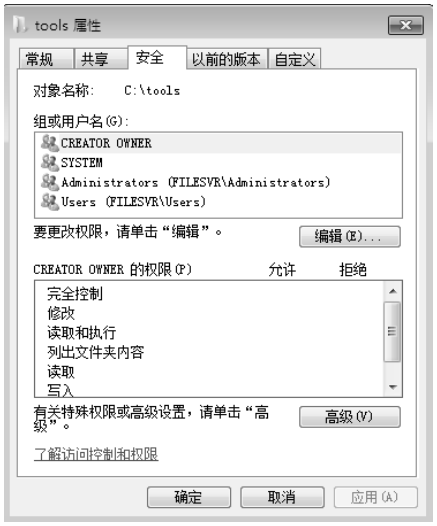


图 3-2　文件夹安全

图 3-3　本地连接属性

STEP2 在“tools 的权限”对话框中设置 userA 的权限为“读取和执行”，如图 3-4 所示。采用同样办法，设置 userB 的权限为“修改”，如图 3-5 所示。

图 3-4　设置 userA 的权限

图 3-5　设置 userB 的权限

STEP3 以用户账户名 userA 登录计算机，可以访问 tools 文件夹，浏览文件内容，修改文件内容后在保存时会出现“拒绝访问”提示，并且不能在文件夹中新建文件。以用户账户名 userB 登录计算机后，同样可以访问 tools 文件夹，浏览文件内容，还可以修改文件，建立新文件。

3.2.2　权限的组合

如果一个用户同时属于多个组，而且当该用户与这些组分别对某文件或文件夹拥有不同的权限设置时，则该用户对这个文件的有效权限是分配给用户账户的权限和用户所属各组的

权限的累加。

userA 用户属于本地组 tech 和 sale，管理员创建一个文本文件 file.txt，设置本地组 tech 对它的权限为读取，本地组 sale 对它的权限为写入，用户 userA 对它的权限为读取和执行，此时用户账户 userA 对文件 file.txt 的最终权限为“读取+写入+执行”。

3.2.3　权限的继承

新建的文件或者文件夹会自动继承上一级目录或磁盘分区的 NTFS 权限，访问控制项中有灰色对勾的选项是继承来的，如图 3-6 所示，不能直接修改从上一级继承来的权限。

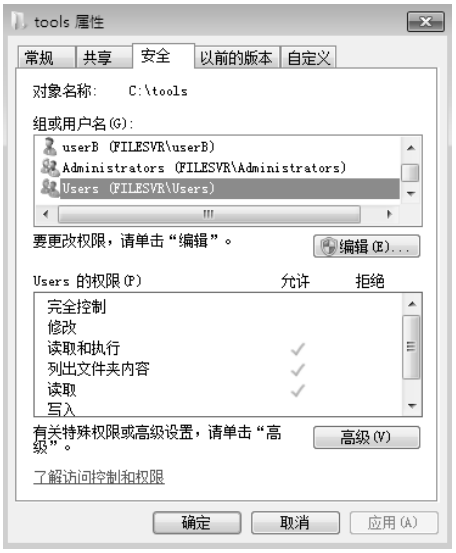


图 3-6　继承的权限

对于一些要设置单独 NTFS 权限的文件或文件夹，不需要从上一级继承权限，可以将继承来的权限删除，然后重新设置 NTFS 权限，步骤如下所述。

STEP1 右键单击 tools 文件夹，选择“属性”，在“tools 属性”对话框中选择“安全”选项卡，单击“高级”按钮，出现“tools 的高级安全设置”对话框，如图 3-7 所示。

图 3-7　tools 的高级安全设置

STEP2 在“tools 的高级安全设置”对话框单击“更改权限”按钮，出现如图 3-8 所示的“权限”选项卡。清除“包括可从该对象的父项继承的权限”选项，清除后系统会提示以前从上一级继承下来的权限是保留还是全部删除，添加或删除继承权限如图 3-9 所示。

图 3-8 “权限”选项卡

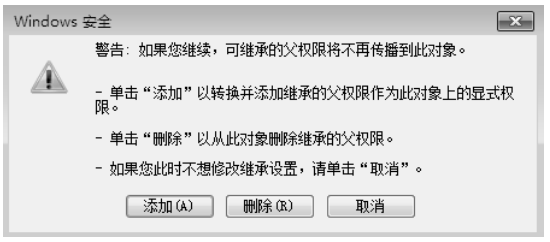


图 3-9 添加或删除继承权限

STEP3 如果保留继承权限则单击“添加”按钮，如果不保留则单击“删除”按钮，删除后，可以自行添加相应的权限。

注意：

图 3-8 所示“权限”选项卡中的“使用可从此对象继承的权限替换所有子对象权限”选项，可以强制下级文件夹或文件继承当前文件夹的权限。

3.2.4 权限的拒绝

由于用户会累加其所属组权限，所以可能造成虽然没有直接为用户分配权限，但用户仍然能够访问文件的情况。只要为用户或其所属的一个组设置拒绝权限，用户将不会拥有访问权限，拒绝权限的优先级高于其他权限。

userA 用户属于本地组 tech 和 sale，管理员创建一个文本文件 file.txt，设置本地组 tech 对它的权限为读取，本地组 sale 对它的权限为写入，用户 userA 对它的权限为拒绝写入，如图 3-10 所示。此时用户账户 userA 对文件 file.txt 的写入权限被“拒绝”。

图 3-10　拒绝用户写入权限

3.2.5　用户的最终有效权限

如果用户同时属于多个组，而某个文件夹或文件对这些组设置了不同的权限，要想快速判断用户对该文件或文件夹的有效权限，步骤如下所述。

STEP1 在如图 3-7 所示的“tools 的高级安全设置”对话框中选择“有效权限”选项卡，如图 3-11 所示。

图 3-11　有效权限

STEP2 单击“选择”按钮，在弹出的对话框中添加 userA 账户，单击“确定”按钮，显示出 userA 对文件夹 tools 的有效权限，如图 3-12 所示。使用同样方法，再查看用户 userB 对 tools 文件夹中文件的有效权限。

图 3-12　userA 的有效权限

3.2.6　取得所有权

NTFS 磁盘内的每个文件和文件夹都有所有者，默认情况下，创建文件或文件夹的用户就是该文件或文件夹的所有者。所有者可以更改其所拥有的文件或文件夹的权限，使其他用户无法访问。管理员可以通过特殊权限，取得文件或者文件夹的所有权，再重新设置权限。

ABC 公司的 userB 用户将计算机上的文件夹 soft 设置为只有自己有完全控制的权限，其他人无任何权限，如图 3-13 所示。userB 离职后，网络管理员删除了他的用户账户，但他计算机上文件夹 soft 管理员也无法访问，管理员使用以下步骤解决这个问题。

STEP1 以管理员 Administrator 账户登录，找到文件夹 soft，右键单击文件夹，选择“属性”→“安全”，出现如图 3-14 所示的对话框，表示当前用户没有权限查看或编辑。

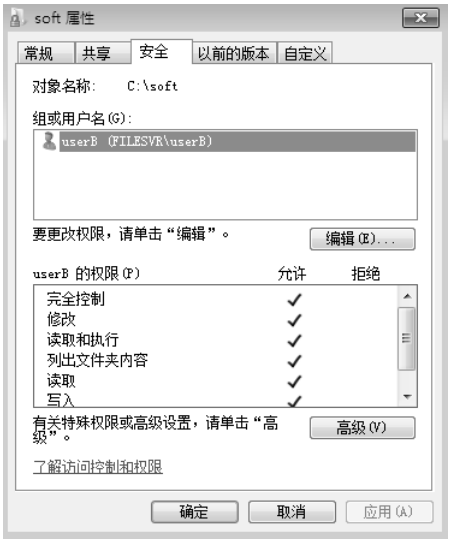


图 3-13　userB 完全控制

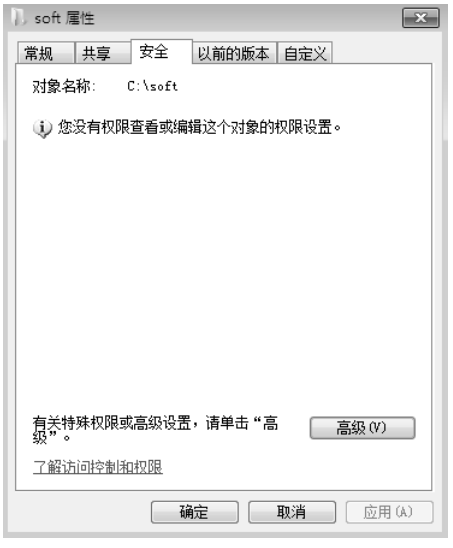


图 3-14　管理员无权查看

STEP2 在图 3-14 所示的对话框中单击“高级”按钮，选择“所有者”选项卡，无法显示当前的所有者，如图 3-15 所示，单击“编辑”按钮。

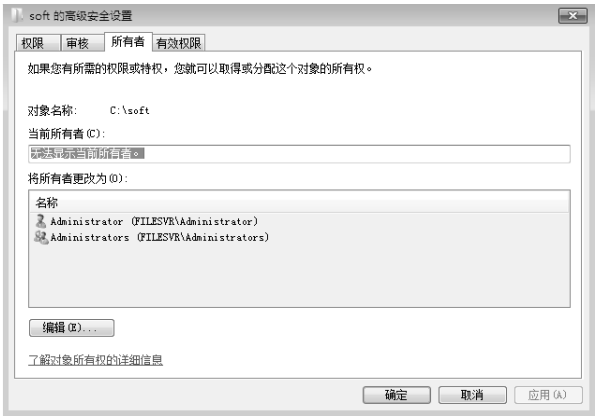


图 3-15　“所有者”选项卡

注意:

必须在“用户账户控制”功能关闭的情况下才能出现图 3-15 所示的对话框，否则会要求输入系统管理员账户与密码。“用户账户控制”功能设置方法为“开始”→“控制面板”→“用户账户”→“更改用户账户控制设置”，改为“从不通知”，此项设置要重新启动计算机后生效。

STEP3 在“所有者”选项卡中，选择将所有者更改为哪个用户或组，这里有默认的用户 Administrator 和组 Administrators。这里选择前者，确定后弹出安全提示窗口，单击“确定”按钮，如图 3-16 所示。再次查看 soft 的所有者，已经变成 Administrator，如图 3-17 所示。

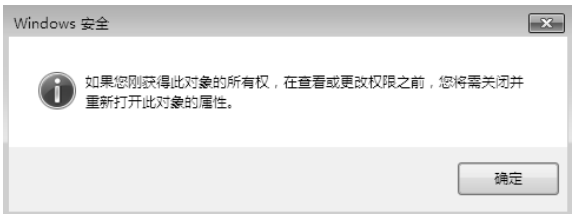


图 3-16　安全提示

图 3-17　soft 的所有者

STEP4 关闭文件夹属性对话框，再次打开“安全”选择卡，单击“编辑”按钮后，可以使用“添加”和“删除”按钮设置权限，如图 3-18 所示。

图 3-18 重新设置 NTFS 权限

3.2.7 移动和复制对权限的影响

当 NTFS 文件系统分区内的文件被复制或移动到另一个文件夹后，其权限可能会发生变化，具体变化情况如表 3-1 所示。

表 3-1 NTFS 文件系统中的文件或文件夹移动和复制权限变化表

复　制	移　动	
继承目的地文件夹权限	在同一分区内	保留原来的权限
	在不同分区之间	继承目的地文件夹权限

- 复制：无论文件或文件夹被复制到同一个或不同 NTFS 磁盘分区内，相当于新建一个文件或文件夹，都将继承目的地 NTFS 权限。例如，如果用户对位于 C:\date 内的文件 file 具有读取权限，对文件夹 C:\tools 具有完全控制权限，当 file 被复制到 C:\tools 文件夹，用户对新文件 file 具有完全控制的权限。
- 移动：如果文件或文件夹被移动到同一个 NTFS 磁盘分区，则仍然保持原来的权限。例如，C:\date 文件夹移动到 C:\tools 文件夹，权限不变。如果文件或文件夹被移动到另一个 NTFS 磁盘分区，则继承目的地权限。

注意：

如果文件或者文件夹从 NTFS 磁盘分区复制到 FAT 分区，NTFS 权限将消失；当需要移动文件或文件夹时，必须对源文件或文件夹具备修改权限，同时也必须对目的文件夹具有写入权限。

3.3　任务 2：访问网络文件

资源共享是网络的主要功能，通过公用文件夹和共享文件夹可以将文件资源共享给网络内的用户。

3.3.1　公用文件夹

磁盘内的文件经过权限设置后，登录计算机的用户可以访问自己有权限的文件，但无法访问其他用户的文件。Windows Server 2008 R2 有一个公用文件夹，在本地登录的用户都可以访问这个公用文件夹，依次打开桌面上的“计算机”→“本地磁盘 C”→“用户”文件夹下的“公用”文件夹，如图 3-19 所示。

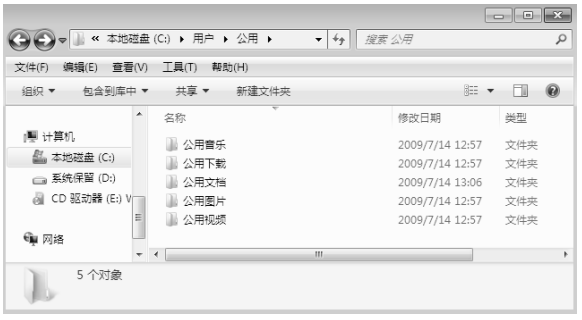


图 3-19　公用文件夹

公用文件夹内默认已经建立公用视频、公用图片等 5 个文件夹，用户只要把欲共享的文件复制到适当的文件夹即可，还可以在公用文件夹内建立更多的文件夹。

如果让用户通过网络访问公用文件夹，需要启用公用文件夹共享。选择“开始”→“控制面板”→“网络和 Internet”→“网络和共享中心”→“更改高级共享设置”，在出现窗口中的“公用文件夹共享”处，选择“启用共享以便可以访问网络的用户可以读取和写入公用文件夹中的文件”，单击“保存修改”按钮，如图 3-20 所示。

图 3-20　启用公用文件夹共享

3.3.2 新建共享文件夹

公用文件夹共享无法针对个别用户，所有用户共享权限是相同的，用户自己创建的共享文件夹可以针对不同用户设置共享权限。

ABC 公司文件服务器上的 tools 文件夹需要在局域网内共享，让网络内的其他用户可以访问，步骤如下所述。

STEP1 右键单击 tools 文件夹，选择“共享”→“特定用户”，如图 3-21 所示。

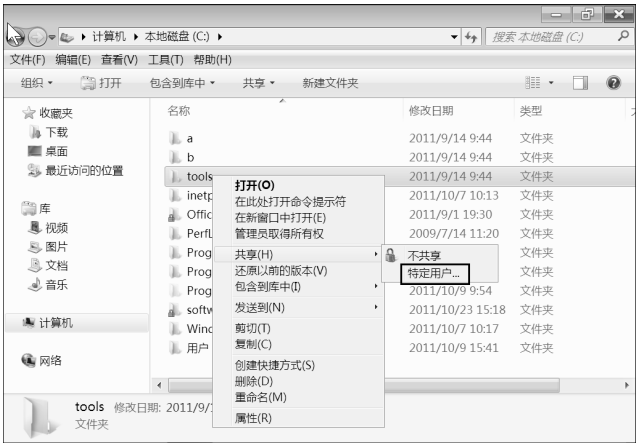


图 3-21 共享文件夹

STEP2 在出现的“文件共享”对话框中选择或输入要与其共享的用户或组名，单击“添加”按钮，如图 3-22 所示。

图 3-22 添加共享用户（1）

STEP3 选择的用户或组的默认共享权限为“读取”，若要更改可单击用户右边的下拉箭头，如图 3-23 所示，然后从显示列表中选择共享权限，单击“共享”按钮。

图 3-23　添加共享用户（2）

STEP4 如果计算机的网络位置是公用网络，则会出现如图 3-24 所示的提示对话框，选择“是，启用所有公用网络的网络发现和文件共享”。

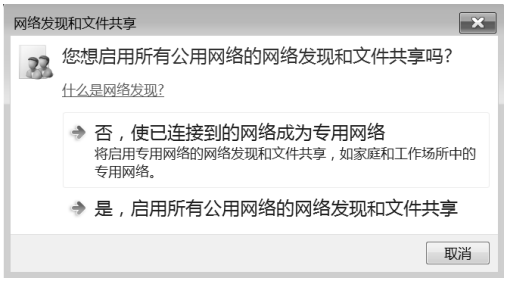


图 3-24　网络发现与文件共享

STEP5 在如图 3-25 所示的对话框中单击“完成”按钮。

图 3-25　文件共享

注意:

只有 Administrator 组内的成员有创建共享文件夹的权限，普通用户在共享文件夹时，需要输入系统管理员账户和密码后才能共享。

创建共享文件夹或更改共享权限，还可以通过文件夹“属性”对话框来实现，在如图 3-26 所示的文件夹“tools 属性”对话框的“共享”选项卡中，单击“共享”按钮，也会打开图 3-22 所示的添加共享用户的对话框，也可以单击“高级共享”按钮，弹出如图 3-27 所示的对话框，选中“共享此文件夹”，设置共享名称，单击“确定”按钮。共享名是在网络上查看此共享文件夹时看到的名称，此名称可以和文件夹名称相同或不同，一个文件夹可以建立多个共享名称。

图 3-26 “共享”选项卡

图 3-27 高级共享

3.3.3 访问共享文件夹

在服务器上创建共享文件夹后，客户端可以通过各种方式访问共享文件夹，通常情况下使用以下 3 种方式。

1. 使用 UNC 路径

UNC 是 Universal Naming Convention 的缩写，意为统一命名约定。UNC 路径的格式是“\\服务器名称\ 共享名”，或者是“\\服务器 IP 地址\ 共享名”。

在客户机上选择“开始”→“运行”，输入 UNC 路径，确定后就可以查看共享资源。如图 3-28 所示。也可以在“资源管理器”或者 IE 浏览器地址栏中输入 UNC 路径，来访问网络中的共享文件夹。如果登录本机的用户对网络上的共享文件夹没有访问权限，在使用 UNC 路径访问共享文件夹时，系统会提示用户输入有权限的用户名和密码，在如图 3-29 所示的对话框中输入有访问权限的用户名和密码，才可以访问服务器上共享的文件夹。

图 3-28　输入 UNC 路径

图 3-29　输入用户名和密码

2．利用“网络发现”连接网络计算机

客户端计算机启用网络发现功能后，可以自动查找到共享文件夹。选择“开始”→“控制面板”→“网络和 Internet”→“网络和共享中心”→“高级共享设置”，打开如图 3-30 所示的窗口，选择“启用网络发现”，单击“保存修改”按钮。

图 3-30　启用网络发现

双击桌面上的“网络”图标，会显示网络中的计算机列表，双击计算机名，会显示该计算机上共享的文件夹，如图 3-31 所示。

图 3-31　通过“网络发现”浏览共享

3．利用网络驱动器来连接网络计算机

对于一些经常访问的共享文件夹，可以将其映射为本地的一个驱动器，访问时就象访问本地驱动器一样，只不过网络驱动器上的文件不在本机上，而在网络中的计算机上。

STEP1 双击桌面的“计算机”图标，打开“计算机”窗口，选择“工具”菜单的“映射网络驱动器”项，如图 3-32 所示。

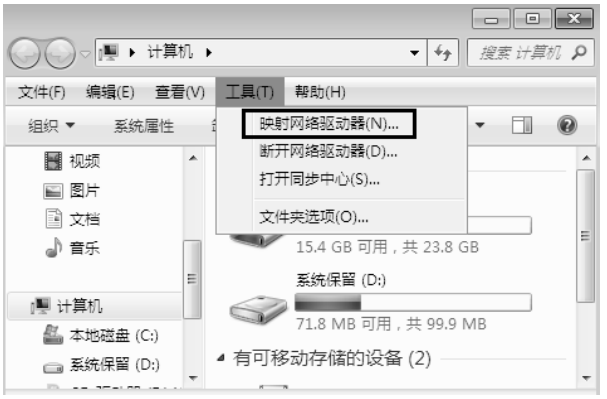


图 3-32　映射网络驱动器

STEP2 在“映射网络驱动器”页面选择驱动器号，单击“浏览”按钮选择需要映射的共享文件夹或直接输入共享文件夹的 UNC 路径，单击“完成”按钮，tools 映射网络驱动器 Z 如图 3-33 所示。

图 3-33　tools 映射网络驱动器 Z

STEP3 完成上述操作后，可以通过桌面上的“计算机”图标来访问共享文件夹，如图 3-34 所示的 Z 驱动器为网络驱动器。

图 3-34　访问网络驱动器 Z

3.3.4　隐藏共享文件夹

共享的文件夹可以被网络上所有用户查看到，尽管其可能没有任何操作权限。如果希望共享文件夹在用户访问服务器时不显示，需要将共享文件夹隐藏起来。只要在共享名后面加上一个“$”符号，就可以隐藏共享。

系统已经自动建立了多个隐藏的共享文件夹，它们是供系统内部使用或系统管理用的。选择“开始”→“管理工具”→“共享和存储管理”，打开如图 3-35 所示的窗口。其中，ADMIN$、C$、D$和 IPC$为系统自动建立的隐藏共享文件夹，tools$为用户创建的隐藏共享文件夹。

- ADMIN$：计算机远程管理期间使用的资源。
- C$、D$：允许管理员连接到驱动器根目录下的共享资源。
- IPC$：共享命名管道的资源，利用它可以与目标主机建立连接，并远程进行日常管理和维护。

在网络中看不到隐藏的共享文件夹，所以只能利用 UNC 路径或映射网络驱动器来访问隐藏的共享文件夹，例如，\\Filesvr\tools$，或者将\\Filesvr\tools$映射成为本地驱动器。

图 3-35　共享和存储管理

3.4 任务 3：设置共享权限

1. 共享权限

如果用户从网络访问服务器上的文件资源，除需为其分配适当的 NTFS 权限外，还需为其分配共享权限。在如图 3-27 所示的对话框中单击“权限”按钮，弹出如图 3-36 所示的设置共享权限对话框，通过允许和拒绝复选框来控制用户和组通过网络访问共享文件夹的权限。共享权限比 NTFS 权限少，只有读取、更改和完全控制这 3 种。

- 读取：查看文件名及子文件夹名，查看文件中的数据，运行程序文件。
- 更改：除了读取权限，还能够新建与删除文件和子文件夹，更改文件内的数据。
- 完全控制：除了以上两种权限，还具有更改权限（只适用于 NTFS 文件系统内的文件或文件夹）。

图 3-36　共享权限

2. 共享权限与 NTFS 权限

如果共享文件夹处于 NTFS 分区，用户通过网络访问共享文件的最终有效权限取两者之中最严格的设置。例如，用户 A 对共享文件夹“C:\test”的共享权限为“读取”，NTFS 权限为“完全控制”，则用户 A 对“C:\test”的最后有效权限为两者中最严格的“读取”。

注意：

共享文件夹权限只对通过网络来访问此文件夹的用户有限制，如果用户由本地登录，则不会受此权限限制。如果 A 用户直接由本地登录，而不是通过网络登录，则用户 A 对 C:\test 的有效权限由 NTFS 权限决定，也就是“完全控制”。

3.5　任务 4：安装和配置打印服务器

打印机是常见的计算机外部设备，其通过 USB 接口或并行线缆等连接至计算机。企业出于成本考虑，一般不会为每个用户配备打印机，而是将打印机设置为办公网络中独立的节点，用户通过网络远程打印。常见的打印解决方案有网络打印机、打印服务器、Windows 打印服务等。

1. 网络打印机

网络打印机带有有线或无线网络接口，直接连接到网络交换机或无线 AP，通过 TCP/IP 协议与计算机通信，如图 3-37 所示。

2. 打印服务器

如果企业已经购置了不含网络接口的打印机，可以购买如 3-38 所示的打印服务器。有些打印服务器带有网络接口，用于连接网络，还有些打印服务器带有 USB 接口，用于连接不含网络接口的打印机。

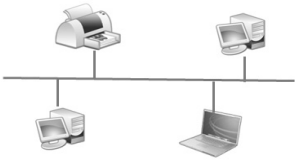


图 3-37　网络打印机拓扑

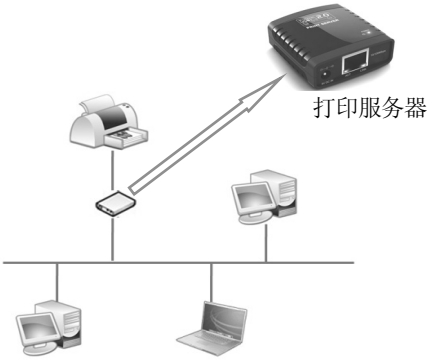


图 3-38　打印服务器拓扑

3. Windows 打印服务

使用 Windows 中的打印服务可以在网络上共享打印机，而且可以使用“打印管理”控制台管理单元集中执行打印管理任务，监视打印队列，并在打印队列停止处理打印作业时接收通知，Windows 共享打印机拓扑如图 3-39 所示。

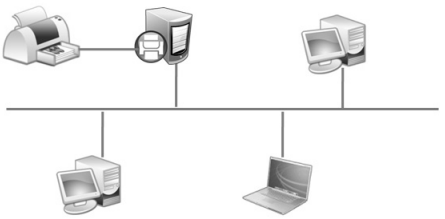


图 3-39　Windows 共享打印机拓扑

3.5.1 安装打印机

可安装的打印机有本地打印设备和网络打印设备两种，本地打印设备可以通过 LPT 或者 USB 接口连接，网卡接口的打印机可以通过网卡连接。网络用户在连接共享打印机时必须安装网络打印机。

1．安装本地打印机

STEP1 选择“开始”→“设备和打印机”，在添加设备和打印机窗口选择“添加打印机”，打开如图 3-40 所示的对话框，单击“添加本地打印机”。

图 3-40 添加打印机

STEP2 在“选择打印机端口”页面选择打印机端口，一般是 LPT1，单击“下一步”按钮，如图 3-41 所示。

图 3-41 选择打印机端口

STEP3 在“安装打印机驱动程序”页面选择打印机厂商与打印机型号，单击“下一步”按钮，输入打印机名称，安装打印驱动程序，如图 3-42 所示。

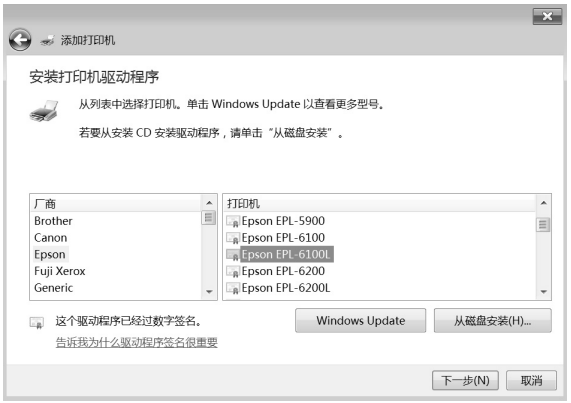


图 3-42　选择厂商和打印机型号

STEP4 在“打印机共享”页面选择是否共享打印机，如果共享则设置打印机共享名称，单击“下一步”按钮，如图 3-43 所示。

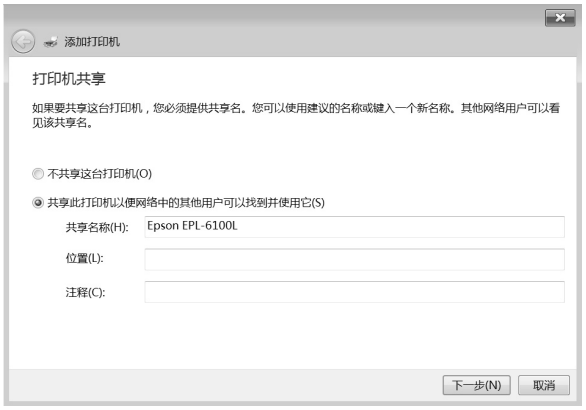


图 3-43　设置共享名称

STEP5 显示成功添加打印机，也可以单击“打印测试页”按钮来测试是否可以正常打印，如图 3-44 所示，单击“完成”按钮，完成本地打印机添加操作。

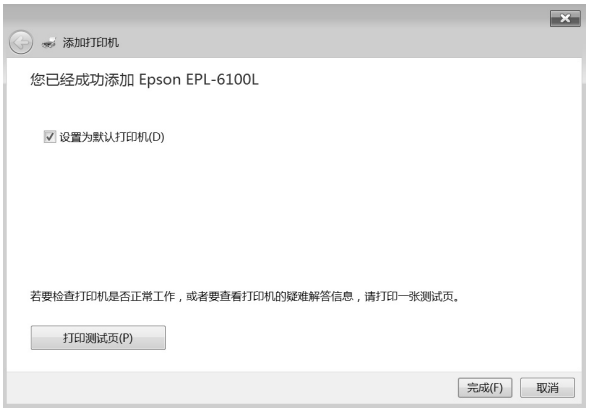


图 3-44　成功添加打印机

如果安装的是具有网卡接口的打印机，与安装本地打印机的步骤相似，只是在图 3-41

中选择“创建新端口”，在端口类型处选择“Standard TCP/IP Port”后，单击“下一步”按钮，输入打印机名称或 IP 地址和端口名称，接下来的步骤与添加本地打印机相同。

2．安装网络打印机

STEP1 在如图 3-40 所示的“添加打印机”对话框中单击“添加网络、无线或 Bluetooth 打印机（W）”。

STEP2 在“搜索可用打印机”页面搜索到网络中共享的打印机，如图 3-45 所示。

STEP3 选择要添加的网络打印机，单击“下一步”按钮，安装打印机驱动程序，如图 3-46 所示，显示添加成功后，单击“下一步”按钮，完成添加操作。

在 STEP2 中，如果要连接的打印机未出现，可以单击“我需要的打印机不在列表中”，将出现如图 3-47 所示的对话框，可以通过 3 种方式连接共享打印机，完成后单击“下一步”。其他步骤与添加本地打印机相同。

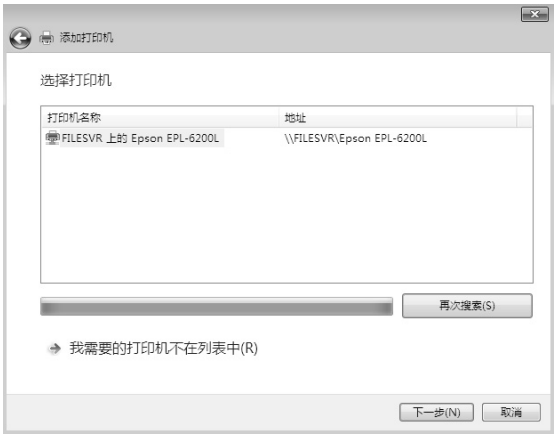


图 3-45　搜索网络打印机

图 3-46　安装网络打印机驱动程序

图 3-47　按名称或 IP 地址查找打印机

3.5.2　配置打印机属性

打印机安装完成后，需要对打印机做进一步设置，以便其更好地为用户提供服务。

1．设置打印优先级

公司内部有一台同时对基层员工和部门主管提供服务的打印设备，希望部门主管的文件优先打印。一般情况下，打印的顺序是按照时间的先后顺序，可以通过打印优先级的调整来改变打印顺序。

STEP1 在打印服务器上为一台物理打印机添加两台逻辑打印机，即重复添加此打印机，一台名为 Printer1，另一台名为 Printer2。

STEP2 选择“开始”→“设备和打印机”，在打印机上右键单击（两台逻辑打印机被合并到一个图标内），选择“打印机属性”→“Printer1”（要改变优先级的打印机），如图 3-48 所示。

图 3-48　打印机属性

STEP3 在“Printer1”属性对话框中选择“高级”选项卡，将 Printer1 的优先级设置为 1。采用同样方法，将 Printer2 的优先级设置为 99。这里的 1 代表最低优先级，99 代表最高优先级，发送到 Printer2 的打印作业将优先打印，如图 3-49 所示。

图 3-49　改变优先级

2．设置打印机池

打印机池是由多台打机组成的一台逻辑打印机，用户可以像使用一台打印机一样进行打印。当用户将文件发到此打印机时，打印机会根据打印设备的忙碌状态来决定要将此文件发到打印机池中的哪一台打印设备打印。

如图 3-50 所示计算机的 LPT1 和 LPT3 上分别连接一台打印机，这两台打印机对应一台逻辑打印机，选中“启用打印机池”选项，然后在端口中选择“LPT1”和“LPT3”，单击“确定”按钮。

图 3-50　启用打印机池

3．使用后台打印

后台打印的作用是先将收到的文件保存在磁盘内，然后将其发送到打印机设备打印。将文件发往打印设备的工作由缓冲器负责，并且在后台运行。在打印机属性对话框的“高级”选项卡中可以选择“立即开始打印”或者是“在后台处理完最后一页时开始打印”。

3.5.3　设置打印机权限

在打印机属性对话框的“安全”选项卡里，可以看到所有分配权限的用户列表，选中某个用户或组，会列出为此用户或组分配的权限，常用权限有打印、管理打印机和管理文档，如图 3-51 所示。

- 打印：如果为用户分配打印权限，用户就可以连接到此打印机，并可以将文档发送到打印机。默认情况下，Everyone 组具有打印权限，即任何用户都具有打印权限。
- 管理文档：可以对发送到打印机的打印作业进行暂停、继续、重新开始和取消等操作。默认情况下，系统为 CREATOR OWNER 组分配了管理文档权限，当用户发送打印作业到打印机时，只对自己发送的打印作业具有管理文档权限。
- 管理打印机 ：用户可以对打印机进行日常的管理操作，如更改打印机名称、设置打印共享、设置打印机端口、设置打印机的优先级、管理打印机权限及暂停或重启打

印机等操作。默认情况下，Administrator 和 Administrators 组的成员具有管理打印机的权限。

注意：

如果要将共享打印机隐藏起来，让用户无法通过网络浏览到它，只要将共享名的最后加一个符号$即可。对于被隐藏起来的打印机，用户还可以通过自行输入 UNC 网络路径的方式连接。

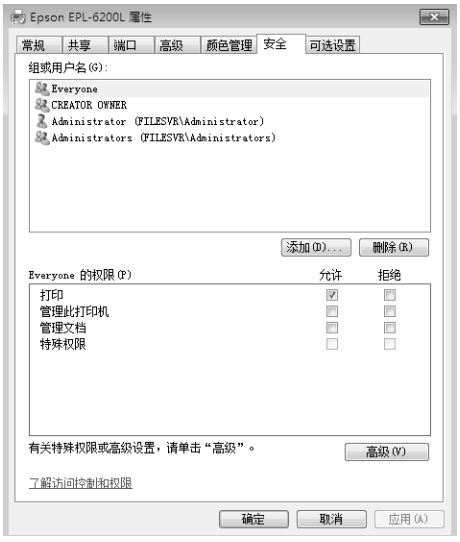


图 3-51 “安全”选项卡

3.6 实训

实训环境一

HT 公司有员工 Lisi 离职，网络管理员删除了他的用户账户 Lisi。后来发现他的计算机上某些重要的文件夹谁都访问不了，网络管理员如何才能访问该文件夹并重新为该文件夹设置 NTFS 权限？公司有一台系统为 Windows Server 2008 R2 的文件服务器，D:\software 中存放着公司常用的软件，user1 和 user2 等普通用户对其拥有读取权限，Administrator 对其拥有完全控制权限，现在要将 D:\software 中的数据移动到 E 分区，如何能保证权限不变？

需求描述

- 管理员账户 Administrator 取得 Lisi 文件夹的所有权。
- 设置 Administrator 账户的 NTFS 权限。
- 配置 E 分区的 NTFS 权限。
- 将 software 移动到 E 分区。

实训环境二

HT 公司网络采用工作组模式，网络中文件服务器上创建了 3 个共享文件夹，其中

software 文件夹用于向全体员工提供常用软件，product 文件夹用于存放生产部的相关资料，finance 文件夹用于存放财务部的相关资料。

需求描述

- 创建共享文件夹 software 并配置权限，使所有用户具有读取权限，而管理员具有完全控制权限。
- 创建共享文件夹 product 并配置权限，使生产部的员工具有修改权限，而其他用户无任何权限。
- 创建共享文件夹 finance 并配置权限，使财务部的员工具有修改权限，而其他用户无任何权限。

实训环境三

HT 公司网络中有一台系统为 Windows Server 2008 R2 的打印服务器 Prtsvr，该服务器上连接着一台打印设备，希望该服务器为全体员工提供打印服务，且部门经理较普通员工有优先打印权限。

需求描述

- 添加两台本地打印机 Prtsvr1 和 Prtsvr2。
- 配置打印权限，使普通员工在 Prtsvr1 上具有打印权限，部门经理在 Prtsvr2 上具有打印权限。
- 配置打印优先级，使部门经理优先于普通员工打印。

3.7 习题

- NTFS 文件系统与 FAT32 相比有什么优势？如何获得 NTFS 分区？
- 在相同分区和不同分区内，复制和移动文件 NTFS 权限有什么变化？
- 如何隐藏共享文件？如何访问隐藏共享文件？
- 共享权限有哪些？分别具有什么权限？
- 打印设备与打印机有什么区别？
- 打印机权限有哪些？如何设置打印机权限？

第 4 章

创建 Active Directory 域

项目需求：

ABC 公司规模迅速扩大，成立多个部门，网络中增加了 100 台计算机，公司要集中管理计算机和用户账户以及其他网络资源，需要将网络变成域结构，把所有的计算机加入域。管理员要按照部门来管理用户账户和组，工作量较大，考虑要在每个部门委派一个员工协助管理本部门的员工账户和密码。

技能目标：

- 理解域和活动目录的概念
- 理解域的结构
- 会创建 Windows 域
- 会将计算机加入域或脱离域
- 会管理域组和域用户
- 会管理 OU

MEMO

4.1 知识介绍——域和活动目录

在小型网络中，管理员通常独立管理每一台计算机，当网络规模扩大到一定程度后，许多管理工作需要在每台计算机上重复做多遍。此时可以将网络中的多台计算机在逻辑上组织在一起，视为一个整体，进行集中管理，这种区别于工作组的网络环境就是域（Domain）。

4.1.1 活动目录和域的概念

1．活动目录（Active Directory）

目录在日常生活中经常用到，能够帮助人们很容易并且迅速地搜索到所需要的数据。活动目录是一种服务，它存储着整个网络内的用户账号、组、打印机和共享文件夹等活动目录对象的相关数据。活动目录不是普通的文件目录，活动目录具有以下特点。

（1）集中管理

活动目录集中组织和管理网络中的资源信息，类似图书馆的图书目录，目录数据库使整个 Windows 网络的配置信息集中存储，管理员可以集中管理网络，提高管理效率。

（2）便捷的网络资源访问

活动目录允许用户一次登录网络就可以访问网络中的所有该用户有权限访问的资源，并且，用户在访问网络资源时不必知道资源所在的物理位置。

（3）可扩展性

活动目录具有强大的可扩展性，目录可以随着公司或组织规模的增长而扩展，从一个网络对象较少的小型网络环境发展成大型网络环境。

2．域和域控制器

域是活动目录的一种实现形式，也是活动目录最核心的管理单位。在域中可以将一组计算机作为一个管理单位，域管理员可以实现对整个域的管理和控制。例如，为用户创建域用户账号，使他们可以登录域并访问域资源，控制用户什么时间在什么地点登录，能否登录，登录后能够执行哪些操作等。一个域由域控制器和成员计算机组成，域网络结构如图 4-1 所示。域控制器（Domain Controller，DC）就是安装了活动目录服务的一台计算机。活动目录的数据都保存在域控制器内，即活动目录数据库。管理员可以通过修改活动目录数据库的配置来实现对整个域的管理和控制，客户机要访问域的资源必须先加入域，通过管理员为其创建的域用户账号登录域，同时也必须接受管理员的控制和管理。

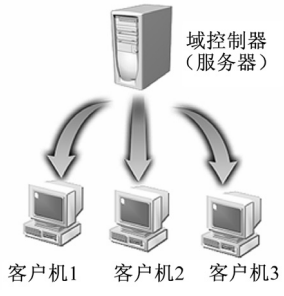


图 4-1 域网络结构

3．域树

当需要配置一个包含多个域的网络时，需要将网络配置成域树结构。域树是一种树形结构，如图 4-2 所示。在图 4-2 所示的域树中，最上层的域名为 abc.com，是这个域树的根域，也称为父域。下面的两个域 sh.abc.com 和 gd.abc.com 是 abc.com 域的子域，3 个域共同构成了这个域树。

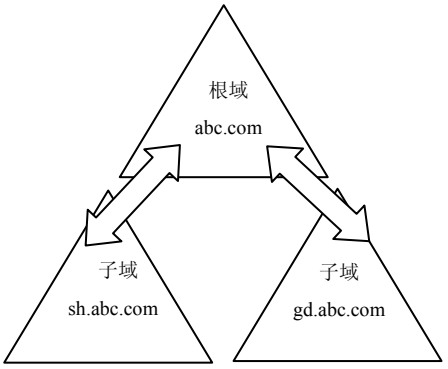


图 4-2　域树

活动目录的域名遵循 DNS 域名的命名规则。在如图 4-2 所示的域树中，两个子域的域名中包含父域的域名，它们的名称空间是连续的，这也是判断两个域是否属于同一个域树的有效手段。

在整个域树中，所有域共享一个活动目录，这个活动目录分散地存储在不同的域中，每个域只负责存储和本域有关的数据，整体上形成一个大的分布式活动目录数据库。在配置一个较大规模的企业网时，可以配置为域树结构，总公司的网络配置为根域，各分公司的网络配置为子域，整体上形成一个域树，以实现集中管理。

4．林

如果网络的规模超大，甚至包含了多个域树，这时可以将网络配置为林结构，也叫作域森林。林由一个或多个域树组成，如图 4-3 所示。林中的每个域树都有唯一的命名空间，它们之间不是连续的。

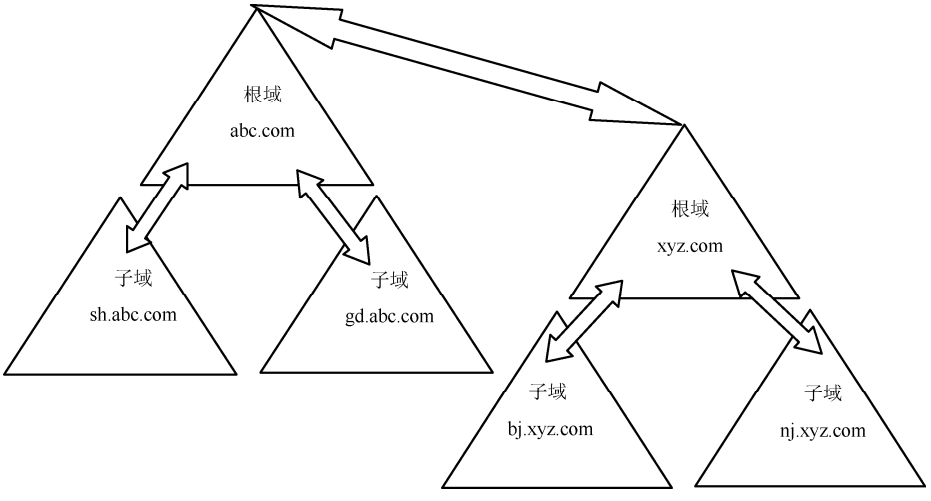


图 4-3　林

在创建林时，组成林的两个域树的树根之间会自动创建相互传递的信任关系。正是因为有了双向的信任关系，使林中和每个域中的用户都可以访问其他域的资源，也可以从其他域登录到本域中。

4.1.2 安装域控制器的条件

创建域必须安装一台域控制器（DC），DC 上存储着域中的资源信息，如名称、位置和特性描述等。通过在一台服务器上安装活动目录，就可将这台计算机安装成 DC。

一台计算机要安装活动目录，必须具备以下条件：

- 安装者必须具备本地管理员权限，普通用户不能安装活动目录。
- 本地磁盘至少有一个分区是 NTFS 文件系统。
- 具有 TCP/IP 设置（IP 地址和子网掩码等）。
- 操作系统版本必须满足条件。在 Windows Server 2008 R2 家族中，除了Windows Web Server 2008 R2和Windows Server 2008 R2 for Itanium-Based Systems，其他都可以扮演域控制器角色。
- 有相应的 DNS 服务器支持以及足够的可用磁盘空间。

4.2 任务 1：安装活动目录

当一台 Windows Server 2008 R2 服务器满足成为 DC 的所有条件时，就可以创建活动目录，步骤如下所述。

STEP1 将计算机名设置为 DC1，IP 地址等设置如图 4-4 所示。

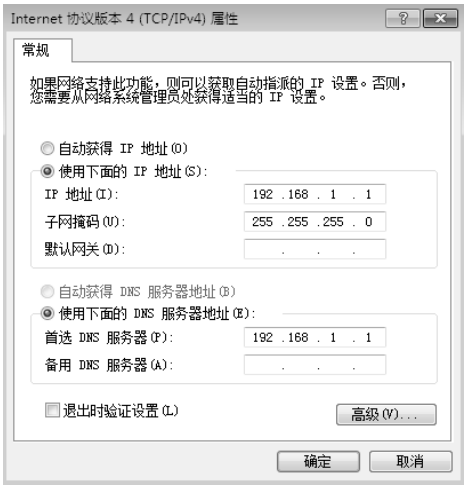


图 4-4 设置 IP 地址

STEP2 选择以下方法之一来安装活动目录。

- 选择“开始”→“管理工具”→“服务器管理器”，或者单击左下角的“服务器管理器”图标。

➘ 选择“开始”→“运行”，输入安装命令“DCPROMO”，单击“确定”按钮，此时会自动执行以下 STEP3～STEP7，然后跳到 STEP8。

STEP3 在“服务器管理器”页面单击“角色”，选择“添加角色”，如图 4-5 所示。

图 4-5　添加角色

STEP4 在“开始之前”页面单击“下一步”按钮，出现“选择服务器角色”页面，在如图 4-6 所示的对话框中选择“Active Directory 域服务”项，接下来单击“添加角色向导”对话框中的“添加必需的功能”按钮安装“.NET Framework 3.5.1，单击“下一步”按钮。

图 4-6　选择服务器角色

STEP5 在“Active Directory 域服务”页面单击“下一步”按钮，接下来在“确认安装选择”对话框中单击“安装”按钮，显示正在安装。

STEP6 安装完成后，单击“关闭”按钮，如图 4-7 所示。

图 4-7　完成安装

STEP7 单击“角色”下的“Active Directory 域服务”，如图 4-8 所示。从对话框中可知，还必须运行 Active Directory 域服务安装向导后，这台服务器才会成为功能完整的域控制器。

图 4-8　Active Directory 域服务

STEP8 单击图 4-8 中的“运行 Active Directory 域服务安装向导（dcpromo.exe）”，出现“Active Directory 域服务安装向导”页面，如图 4-9 所示，单击“下一步”按钮。

STEP9 在操作系统兼容性对话框单击“下一步”按钮，出现“选择某一部署配置”页面，选择“在新林中新建域”，单击“下一步”按钮，如图 4-10 所示。

STEP10 在“命名林根域”页面中输入目录林根域的域名 abc.com，单击“下一步”按钮，如图 4-11 所示。

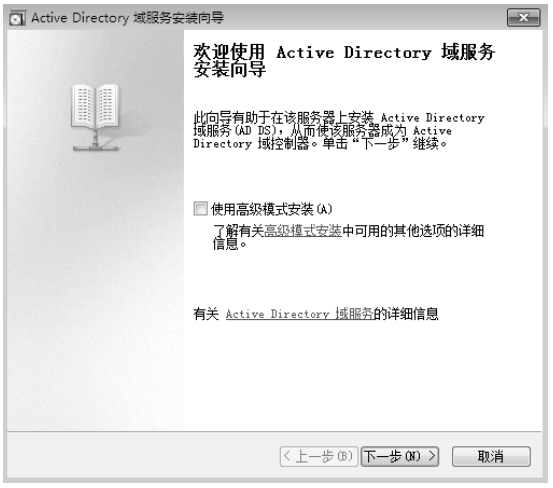


图 4-9　Active Directory 域服务安装向导

图 4-10　选择某一部署配置

图 4-11　命名林根域

STEP11 在设置“林功能级别”页面选择 Windows Server 2008 R2 林功能级别，单击“下一步”按钮，如图 4-12 所示。在接下来出现的对话框中选择“是”。

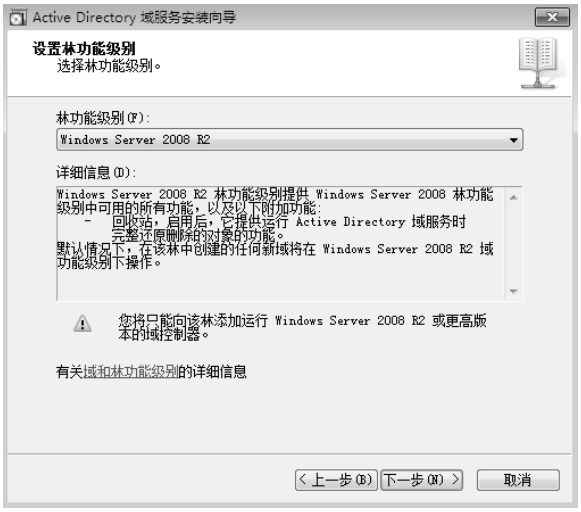


图 4-12　设置林功能级别

STEP12 在如图 4-13 所示的“其他域控制器选项”页面单击“下一步”按钮，会直接在此服务器上安装 DNS 服务。

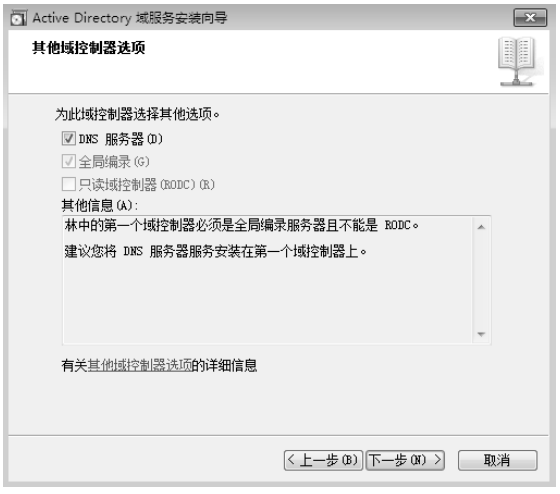


图 4-13　其他域控制器选项

STEP13 在如图 4-14 所示的页面中接受默认的位置，单击“下一步”按钮。

- 数据库文件夹：用来存储 Active Directory 数据库。
- 日志文件文件夹：用来存储 Active Directory 的更改日志，此日志文件可用来修复 Active Directory。
- SYSVOL 文件夹：用来存储域共享文件，必须位于 NTFS 文件系统的磁盘内。

图 4-14　数据库、日志文件和 SYSVOL 的位置

STEP14 在如图 4-15 所示的“目录服务还原模式的 Administrator 密码”页面中输入并确认一个密码，然后单击“下一步”按钮。目录服务还原模式是一个安全模式，进入此模式可以修复 Active Directory 数据库。在系统启动时按 F8 键可选择进入此模式，此时必须输入本步骤所设置的密码。

图 4-15　目录服务还原模式密码

STEP15 在“摘要”页面单击“下一步”按钮，开始安装和配置 Active Directory 服务，如图 4-16 所示。完成后，依据提示需要重新启动系统。

注意：

如果要删除活动目录，可以将域控制器降级为普通的服务器，与升级为域控制器的做法相同，一般采用运行 dcpromo 命令，按照提示完成删除。在操作过程中，系统会提示当前域控制器是否为此域的最后一台域控制器，还会提示输入降级以后普通服务器的管理员账户密码。

图 4-16　配置 Active Directory 服务

4.3　任务 2：将计算机加入域

在完成 Active Directory 安装后，需要将客户机或其他服务器加入域中。用户必须在客户机上拥有管理权限才能将其加入域中。在加入域之前，首先检查客户机的网络配置，确保客户机与域控制器互相连通，配置 IP 地址及首选 DNS 服务器地址。首选 DNS 服务器地址通常配置为第一台 DC 的 IP 地址。以 Windows Server 2008 R2 计算机为例，通过以下步骤将计算机加入域（本例中 DC 的 IP 地址为 192.168.1.1）。

STEP1　将该计算机名设置为 Client01，IP 地址设置为 192.168.1.2，首选 DNS 服务器地址为 192.168.1.1，加入域后计算机名自动改为 Client01.abc.com。

STEP2　在桌面上右键单击“计算机”图标，选择“属性”，单击“更改设置”，在“系统属性”对话框的“计算机”选项卡中单击“更改”按钮，出现如图 4-17 所示的“计算机名/域更改”对话框，输入域名后单击“确定”按钮。

图 4-17　计算机名/域更改

STEP3　在如图 4-18 所示的“Windows 安全”对话框中输入域管理员账户和密码，单击“确定”按钮。

STEP4　出现欢迎加入域的提示，如图 4-19 所示，单击“确定”按钮，根据提示重新启动计

算机，重启后该计算机成功加入了域。

图 4-18　输入域管理员账户和密码

图 4-19　欢迎加入域

注意：

当按照加入域的办法将计算机加入到某个工作组时，就会自动从域中退出。

如 STEP3 不出现输入域管理员账户和密码，而出现错误警告，请检查 TCP/IPv4 处的首选 DNS 服务器是否设置了正确的地址。

4.4　任务 3：域用户账户的管理与应用

如果用户要访问一个基于 Windows Server 2008 R2 的活动目录网络资源，则需要一个合法的域用户账户，在 DC 上可以创建用户账户、组等活动目录对象。与工作组中的本地用户账户相比，域用户账户集中存储在 DC 上，而不是存储在每台成员计算机上。

4.4.1　创建域用户账户

STEP1 选择“开始”→“管理工具”→“Active Directory 用户和计算机”，打开如图 4-20 所示的窗口。右键单击“Users”，选择“新建”→“用户”。

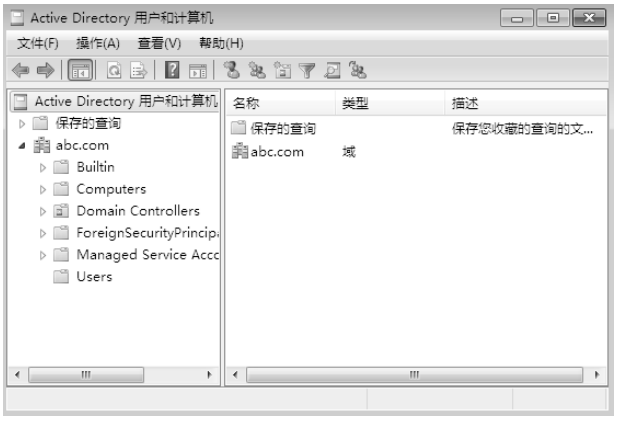


图 4-20　“Active Directory 用户和计算机”窗口

STEP2 在如图 4-21 所示的新建用户对话框中输入用户姓名等相关信息，单击“下一步”按钮。

图 4-21　创建新用户

STEP3 在设置密码对话框中，指定用户账户的密码并选择相应的密码选项，如图 4-22 所示。域用户账户的密码可以由字母、数字和符号组成，并区分大小写，默认必须至少 7 个字符。后续步骤与创建本地用户账户方法相同，按向导提示完成。

图 4-22　设置密码

注意：

在服务器没有升级为域控制器之前，原本位于本地安全数据库内的本地账户，会在升级后被转移到 Active Directory 数据库内，而且是放到 Users 容器内。

4.4.2　配置域用户账户的属性

每个域用户账户内都有一些相关属性，可以通过双击用户账户的方式或右键单击用户账户选择“属性”来修改或设置属性，如图 4-23 所示。这些选项卡中常用部分与本地用户账户属性相似，请参照设置。

“账户”选项卡可限制账户登录时段和登录的计算机范围。

- 登录时间：用来限制用户登录到域的时间，可以在某些时间段内禁止用户使用域账户登录网络，例如，将用户账户设置为只有周一至周五工作时间可以登录，如图 4-24 所示。

- 登录到：定义了用户可以登录的范围列表，可以选择允许用户账户从所有的计算机上登录，也可以限制用户只能用某些特定的计算机来登录域。如图 4-25 所示设置登录地点。

图 4-23　账户属性

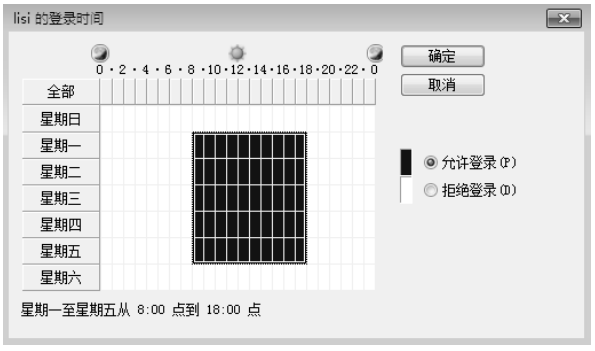


图 4-24　设置登录时间

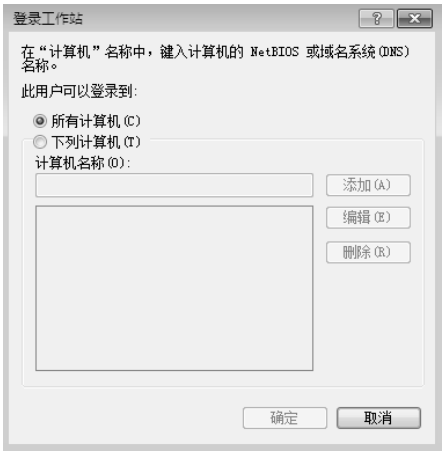


图 4-25　设置登录地点

4.4.3 利用域用户账户登录

域用户可以在域内任何一台非域控制器的计算机上登录域，在登录窗口中单击“切换用户”按钮，再单击“其他用户”，在如图 4-26 所示的登录窗口输入“域名\用户登录名”和密码登录域。

图 4-26 域用户登录

除了域组 Administrators 内的成员，其他一般域用户账户默认无法在域控制器上登录。如果开放一般域用户账户在域控制器上登录的权限，可在域控制器中选择“开始”→“管理工具”→“本地安全策略”，出现如图 4-27 所示的“本地安全策略”窗口，选择“本地策略”→“用户权限分配”，在右侧窗口中双击“允许本地登录”，出现如图 4-28 所示的“允许本地登录属性”窗口，添加允许登录的用户和组。

图 4-27 “本地安全策略”窗口

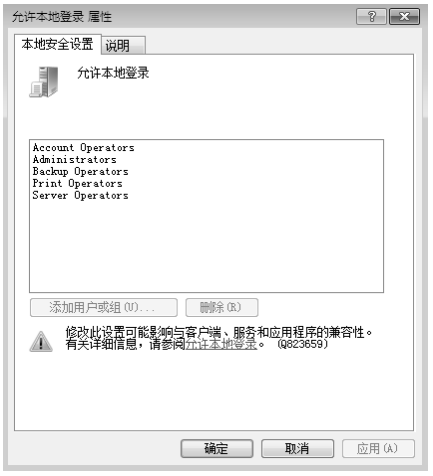


图 4-28 “允许本地登录属性”窗口

4.5 任务 4：域组的管理与应用

域组和本地组的作用相似，是为了向一组用户分配权限以简化用户管理。

4.5.1 域组的类型及使用范围

Active Directory 域内的组有以下两种类型。

- 安全组：管理员一般不为用户账户设置自己独特的访问权限，而是将用户账户加入到相应的安全组中。通过赋予安全组访问资源的权限使得组内用户也具有相应的权限。
- 通信组：通信组没有安全方面的功能，只能用于电子邮件通信，其中可以包含联系人和用户账户。只有在电子邮件应用程序中，才能使用通信组将电子邮件发送给一组用户。

从组的使用范围来看，域组有以下 3 种。

- 本地域组：使用范围是本域，针对本域的资源创建本地域组，其成员可以是用户账户、全局组和通用组，还可能包含相同域内的本地域组，但无法包含其他域内的本地域组。
- 全局组：使用范围是整个林以及信任域。通常使用全局组来管理那些具有相同管理任务或者访问权限的用户账户。
- 通用组：使用范围是整个林以及信任域，与全局组相似。在多域环境中，由于成员信息存储位置不同于全局组，所以通用组成员登录或者查询速度比全局组快。

4.5.2 域组的创建与管理

STEP1 创建域组与创建域用户账户方法类似，在如图 4-20 所示的“Active Directory 用户和计算机”窗口右键单击“Users”，选择“新建”→“组”，输入组名、作用域及类型，单击“确定”按钮，如图 4-29 所示。

图 4-29　创建组

STEP2 双击已创建的组或右键单击组名选择“属性”可修改组信息、添加组成员及所属关系等，如图 4-30 所示。

图 4-30　组的属性

4.6　任务 5：管理组织单位

一个域中有很多种类对象，如用户账户、组、计算机账户、共享文件夹和打印机等，它们的数量很多，组织单位（Organizational Unit，OU）可以将这些对象采用逻辑的等级结构组织起来，方便管理。

OU 是活动目录对象，也是活动目录容器。OU 中可以包含用户和组等对象，也可以在 OU 中建立子 OU。常见的 OU 设计方式如下所述。

- 基于部门的 OU：为了和公司组织机构相同，OU 可以基于公司内部的各种各样的功能部门创建，如财务部和销售部等。
- 基于地理位置的 OU：基于每一个地理位置创建 OU，如北京、上海和广州等。

- 基于对象类型的 OU：在活动目录中将各种对象分类，为每一类对象建立 OU，如用户、计算机和打印机等。

OU 的设计也可以是混合的，例如，可以先在域中创建部门 OU 为“财务部”，然后在“财务部”OU 下创建“用户”OU 和“计算机”OU 两个子 OU，在“用户”OU 中存放本部门所有的用户账号，在“计算机”OU 中存放本部门所有的计算机账户。

在活动目录中默认已经建立了一个名称为 Domain Controllers 的 OU，用于存放域控制器。OU 的图标与其他容器的图标略有不同。

4.6.1　创建和删除组织单位

在“Active Directory 用户和计算机”窗口右键单击域名“abc.com”，选择“新建”→“组织单位”，输入组织单位名称，单击“确定”按钮，如图 4-31 所示。

右键单击已建立的 OU，在快捷菜单中选择相应选项，可以在 OU 下创建其他活动目录对象，或者将现有的活动目录对象移动到 OU 中，如图 4-32 所示。

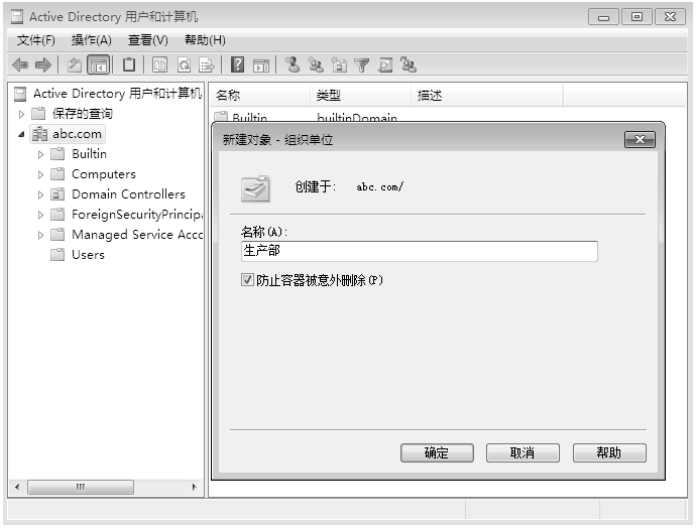


图 4-31　创建生产部 OU

图 4-32　OU 的快捷菜单

如要删除图 4-32 中的“生产部”OU，在快捷菜单中选择“删除”，然后选择确定删除 OU，会出现如图 4-33 所示的警告窗口，提示无法删除。原因是在创建 OU 时，系统默认选中了“防止容器被意外删除”，如图 4-31 所示。可以使用以下操作删除 OU。

图 4-33　警告

STEP1 打开“Active Directory 用户和计算机”窗口，单击“查看”菜单，勾选“高级功能”选项，如图 4-34 所示。

图 4-34　高级功能

STEP2 右键单击“生产部”OU，在图 4-32 所示的快捷菜单中选择“属性”，打开“对象”选项卡，取消勾选“防止容器被意外删除”选项，如图 4-35 所示。单击“确定”按钮，关闭该窗口。

图 4-35　生产部 OU 属性

STEP3 右键单击“生产部”OU，在图 4-32 所示的快捷菜单中选择“删除”，此 OU 成功删除。

4.6.2　组织单位的委派

利用 OU 不但可以有效地组织活动目录对象，还有委派控制和实施组策略的功能。委派控制管理是指管理员可以为适当的用户和组指派一定范围的管理任务，从而减轻管理员的工作负担。

ABC 公司有 5 个部门：人事部、销售部、财务部、技术部和行政部，管理员要按部门来管理用户账户和组；销售部 Sales_OU 中有 3 个用户账户 UserA、UserB 和 UserC，管理员委派 UserA 有权限为本部门员工创建用户账户，重置本部门员工的密码。具体步骤如下所述。

STEP1 创建销售部 Sales_OU，并在该 OU 中创建 UserA、UserB 和 UserC 用户账户，如图 4-36 所示。

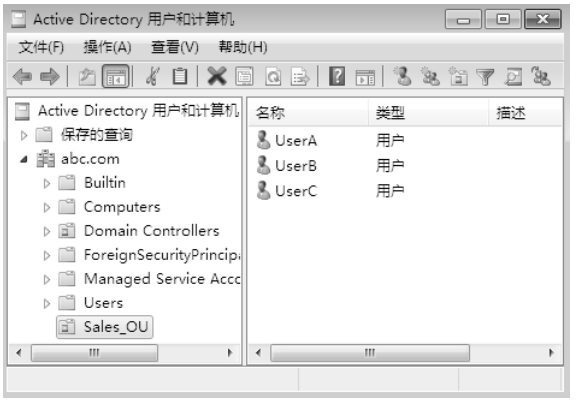


图 4-36　创建 OU 和用户账户

STEP2 右键单击“Sales_OU”，选择“委派控制”，按控制委派向导提示，添加要委派任务的账户 UserA，单击“下一步”按钮，如图 4-37 所示。

图 4-37　添加要委派任务的账户

STEP3 选择要委派的任务，如图 4-38 所示，按向导提示完成委派。

在非 DC（成员服务器）的计算机上执行委派任务，还需要安装“Active Directory 域服务工具”。选择“开始”→“管理工具”→“服务器管理器”，选择“功能”，单击“添加功能”，选择“远程服务器管理工具”→“角色管理工具”→“AD DS 管理单元和命令行工具”和“Active Directory 管理中心”，如图 4-39 所示添加活动目录管理功能。按提示完成安装。

安装完该工具后，可以在非 DC 上使用“Active Directory 用户和计算机工具”。具有委派权限的域用户就可以在自己的计算机上进行委派任务的管理。

图 4-38　选择要委派的任务

图 4-39　添加活动目录管理功能

4.7　实训

实训环境一

HT 公司的网络中约有 100 台计算机，公司需要集中管理计算机和用户账户以及其他网络资源；要建立域环境，域名为 huatian.com。

需求描述

- 在服务器上安装活动目录。
- 将客户机加入到域中。
- 创建域用户和域组。

实训环境二

HT 公司有 5 个部门：技术部、财务部、销售部、人力资源部和生产部，网络管理员需要以部门来管理用户账户和组。网络管理员委派人力资源部的某员工有权限设置本部门员工的密码。

需求描述

- 创建技术部、财务部、销售部、人力资源部和生产部的 OU。
- 在各部门 OU 中创建域用户账户和全局组。
- 设置委派域用户重设密码的权限。

4.8　习题

- 在什么情况下适合采用 Windows 域模式？
- 安装域控制器需要满足哪些条件？
- 活动目录有哪些特点？如何删除活动目录？
- 查找资料，了解漫游用户配置文件的作用及实现方法。

第 5 章

本地安全策略与组策略应用

项目需求：

为了计算机的安全性，ABC 公司要求账户密码长度最少为 8 位，用户连续 3 次输错密码就会被锁定；管理员想查看哪些人曾经访问过文件服务器中的重要数据；所有的普通员工用户登录计算机后不能运行浏览器 Internet Explorer；文件服务器插入 U 盘或光盘不自动播放；公司所有计算机都要安装 Office 办公软件程序，并希望快速部署这个程序；公司要求所有员工在登录计算机时，阅读公司的计算机使用规定。

技能目标：

- 理解本地安全策略
- 会配置账户策略、本地策略、本地组策略
- 理解组策略的作用
- 理解组策略的应用顺序
- 会配置组策略的继承、阻止继承、强制生效、筛选
- 会使用组策略分发软件

MEMO

5.1 知识介绍——本地安全策略

在 Windows Server 2008 R2 系统中，本地安全策略主要包括账户策略和本地策略。本地安全策略影响本地计算机的安全设置，当用户登录到计算机时，就会受到此台计算机的本地安全策略影响。要管理本地安全策略，选择“开始”→“管理工具”→“本地安全策略”，出现如图 5-1 所示的“本地安全策略”窗口，也可以在“开始”→“运行”中输入“secpol.msc”命令。

图 5-1 “本地安全策略”窗口

应用本地安全策略，可以加固系统账户，加强用户密码安全，通过设置“审核对象访问”，跟踪用于访问文件或其他对象的用户账户、登录尝试、系统关闭或重新启动以及类似的事件。

5.2 任务 1：设置账户策略

在网络中，由于用户名和密码过于简单导致的安全性问题比较突出。黑客在攻击网络系统时也把破解管理员密码作为一个主要的攻击目标，账户策略可以通过设置密码策略和账户锁定策略来提高账户密码的安全级别。

5.2.1 密码策略

在如图 5-1 所示的“本地安全策略”窗口中的账户策略下，有“密码策略”和“账户锁定策略”，选择“密码策略”，在右侧出现所有的密码策略内容，如图 5-2 所示。

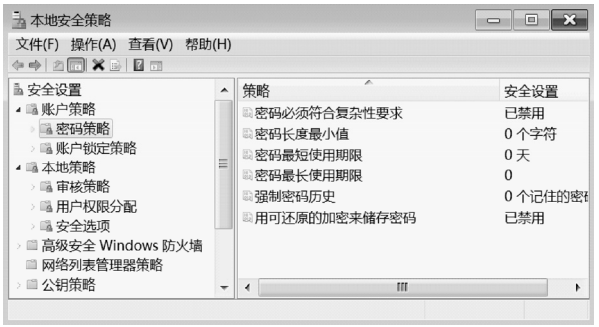


图 5-2 “密码策略”窗口

密码策略中包括以下几个具体策略。

- 密码必须符合复杂性要求：启用此策略后，用户账户使用的密码必须符合复杂性的要求。密码复杂性是指密码中必须包含英文大写字母 A～Z、英文小写字母 a～z、10 个基本数字和特殊符号（例如，−、！、@、$和#）4 类字符中的 3 类字符，并且不少于 6 个字符。双击该策略后，出现如图 5-3 所示的对话框。
- 密码长度最小值：该项安全设置确定用户账户的密码包含的最少字符个数。设置范围为 0～14，将字符设置为 0（默认值），表示用户可以没有密码。双击该策略后，出现如图 5-4 所示的对话框。

图 5-3　密码的复杂性策略

图 5-4　密码长度策略

- 密码最长使用期限：密码使用的最长时间，单位为天。设置范围为 0～999，默认设置为 42 天，如果设置为 0 天，表示密码永不过期。双击该策略后，出现如图 5-5 所示的对话框。
- 密码最短使用期限：此安全设置确定在用户更改某个密码之前至少使用该密码的天数。设置范围为 0～998，如果设置为 0 天，表示可以随时更改密码。期限未到之前，用户不得更改密码，密码最短使用期限必须小于密码最长使用期限。
- 强制密码历史：指多少个最近使用过的密码不允许再使用。设置范围在 0～24 之间，默认值为 0，代表可以随意使用过去使用过的密码。双击该策略后，出现如图 5-6 所示的对话框。
- 使用可还原的加密储存密码：如果应用程序需要读取用户的密码，以便验证用户身份，就可以启用此功能。此策略的应用会使安全性降低，所以一般不要启用。

5.2.2　账户锁定策略

账户锁定策略是指当用户输入错误密码的次数达到一个设定值时，就将此账户锁定。锁定的账户暂时不能登录，只能等超过指定时间自动解除锁定或由管理员手动解除锁定。账户锁定策略包括 3 项设置，如图 5-7 所示。

图 5-5　密码最长使用期限

图 5-6　强制密码历史策略

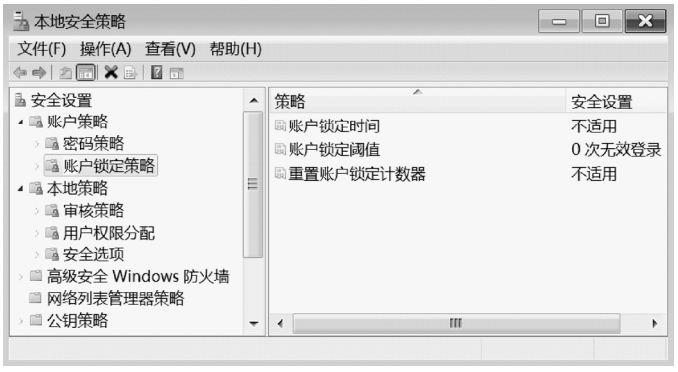


图 5-7　账户锁定策略

- 账户锁定时间：用来设置锁定账户的期限，期限过后自动解除锁定。设置范围为 0～99 999，0 表示永久锁定，不会自动被解除锁定，需要由系统管理员手动解除锁定。
- 账户锁定阈值：用来设置用户几次输入错误密码后登录失败，就将该账户锁定。在未被解除锁定之前，用户无法再使用此账户来登录。设置范围为 0～999，默认值为 0，表示账户永远不会被锁定。
- 重置账户锁定计数器：锁定计数器是用来统计用户登录失败的次数的，起始值为 0，若用户登录失败，则锁定计数的值就会增加 1；若登录成功，则锁定计器的值就会归零。若锁定计数器的值等于账户锁定阈值，该账户就会被锁定。

5.3　任务 2：设置本地策略

本地策略主要涉及是否在安全日志中记录登录用户的操作事件，用户能否交互式登录此计算机，用户能否从网络上访问计算机等。本地策略主要包括审核策略、用户权限分配和安全选项。

5.3.1　审核策略

建立审核跟踪是系统安全的重要内容，通过设置审核策略可以确定是否将计算机中与安全有关的事件记录到安全日志中。另外，也可以将用户登录成功或者失败的信息记录在日志中，以方便查看，审核策略中包括的内容如图 5-8 所示。

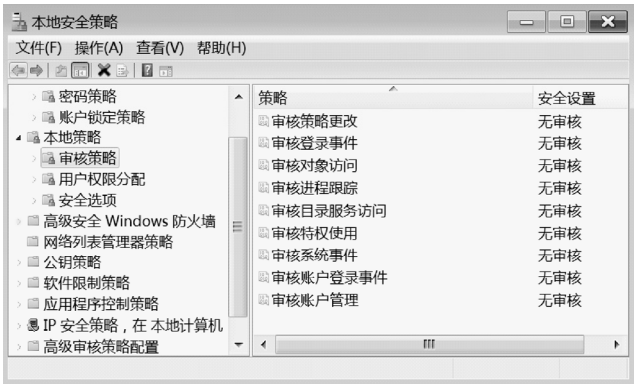


图 5-8　审核策略中包括的内容

审核策略指定了要审核的与安全有关的事件类别，详细的审核策略见表 5-1。

表 5-1　审核策略

审 核 策 略	说　　明
审核策略更改	确定是否对用户权限分配策略、审核策略或信任策略的更改进行审核
审核登录事件	确定是否审核应用此策略的系统中发生的登录和注销事件
审核对象访问	确定是否审核用户访问文件、文件夹和注册表等对象的事件
审核账户登录事件	确定是否审核在这台计算机用于验证账户时，用户登录到其他计算机或者从其他计算机注销的每个实例
审核账户管理	确定是否对计算机上每个账户管理事件进行审核，包括创建、更改、删除用户账户或组，重命名、禁用或启用用户账户，以及设置或更改密码
审核目录服务访问	确定是否对用户访问活动目录服务对象进行审核
审核系统事件	确定是否审核用户重新启动、关闭计算机，以及对系统安全或安全日志有影响的事件

审核策略的安全设置选项包括以下几个方面。

- 成功：当请求的操作成功执行时会生成一个审核项。
- 失败：当请求的操作失败时会生成一个审核项。
- 无审核：相关操作不会生成审核项。

例如，要审核系统中发生的登录和注销事件，双击审核策略中的“审核登录事件”策略，选择“成功”和“失败”，如图 5-9 所示启动审核对象访问策略。

审核的成功与失败记录在事件日志中，失败日志比成功日志更有意义，因为失败通常说明有错误发生。事件查看器用于浏览和管理事件日志，选择“开始”→“管理工具”→“事件查看器”，打开“事件查看器”窗口，如图 5-10 所示。Windows Server 2008 R2 包括两个类别的事件日志：Windows 日志及应用程序和服务日志。

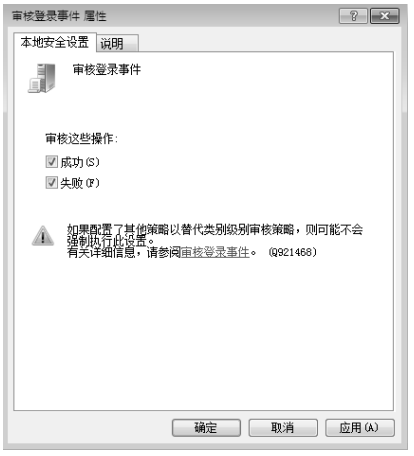


图 5-9　启动审核对象访问策略

图 5-10 “事件查看器”窗口

在“事件查看器”窗口中，事件分为以下几种级别。

- 错误：重要的问题，如数据丢失或功能丧失。例如，如果在启动过程中某个服务加载失败，将会记录“错误”。
- 警告：虽然不一定很重要，但是将来有可能导致问题事件。例如，当磁盘空间不足时，将会记录“警告”。
- 信息：描述了应用程序、驱动程序或服务的成功操作事件。例如，当网络驱动程序加载成功时，将会记录一个“信息”事件。另外，成功的审核和失败的审核也会产生一个“信息”事件，这些审核信息将记录在安全日志中。
- 审核成功：任何成功的已审核的安全事件。例如，用户登录系统成功会被作为“审核成功”事件记录下来。
- 审核失败：任何失败的已审核的安全事件。例如，如果用户试图访问网络驱动器但失败了，则该尝试将会作为“审核失败”事件被记录下来。

Windows 日志中的安全日志主要记录用户登录和对象访问的信息。要查看安全日志，展开“事件查看器”窗口左侧“Windows 日志”→“安全”，可以看到审核成功和审核失败两种事件，如图 5-11 所示。

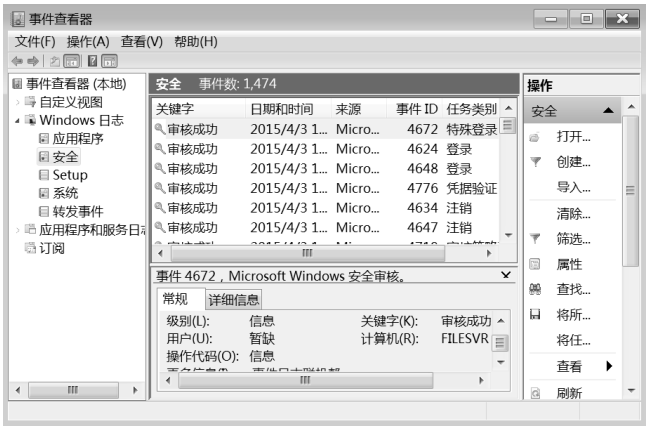


图 5-11　安全日志（1）

双击某一事件，可以查看事件属性，包含更加详细的事件相关信息，如图 5-12 所示。

图 5-12　事件属性

如果日志数量过多，可以利用“操作”菜单中的“清除日志”命令将日志清除，但在清除之前，可以利用“操作”菜单中的“将事件另存为”命令将日志保存。

ABC 公司文件服务器 Filesvr 的文件夹“公司文件”中存放着公司日常工作规范等文档，管理员希望能够查看员工对该文件夹的成功访问和失败访问的情况。

STEP1　在服务器 Filesvr 上选择“开始”→“管理工具”→“本地安全策略”，在“本地安全策略”窗口左侧展开“本地策略”→“审核策略”，双击窗口右侧的“审核对象访问”策略，在“审核对象访问 属性”对话框中选择“成功”和“失败”复选框，如图 5-13 所示，单击“确定”按钮。

STEP2　右侧单击文件夹“公司文件”，选择“属性”，在文件夹属性对话框选择“安全”选项卡，单击如图 5-14 所示的“高级”按钮。

STEP3　在“公司文件的高级安全设置”对话框选择“审核”选项卡，在如图 5-15 所示的对话框中单击“编辑”按钮。

图 5-13　审核对象访问

图 5-14　文件夹属性

图 5-15　公司文件的高级安全设置

STEP4 在如图 5-16 所示的“公司文件的高级安全设置”对话框的审核页面单击“添加”按钮。

图 5-16　审核页面

STEP5 在如图 5-17 所示的“选择用户或组”对话框中添加要审核的用户和组账户，这里添加“Everyone”组，单击“确定”按钮。

STEP6 在“公司文件的审核项目”对话框中选择要审核的项目，单击“确定”按钮，如图 5-18 所示。

图 5-17　选择用户或组

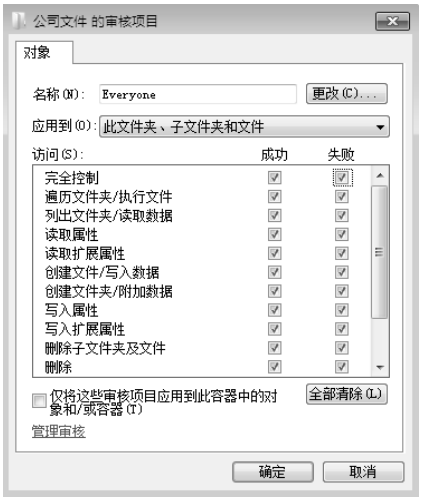


图 5-18　选择审核项目

STEP7 注销当前管理员用户，改用其他用户账户登录，尝试打开被审核的文件。注销后重新使用管理账户登录，选择“开始”→“管理工具”→“事件查看器”，在“事件查看器”窗口展开“Windows 日志”→“安全”，双击图 5-19 中所审核的任务类别为“文件系统”的事件，就可以看到打开文件的操作已被记录。

图 5-19　安全日志（2）

5.3.2　用户权限分配

通过用户权限分配，可以为某些用户和组授予或拒绝一些特殊的权限，如关闭系统、更改系统时间、拒绝本地登录和允许在本地登录等，用户权限分配中的策略如图 5-20 所示。

表 5-2 列出了用户权限分配中的常用安全策略。

图 5-20　用户权限分配中的策略

表 5-2　用户权限分配中的常用安全策略

策　略	说　明
从网络访问此计算机	默认情况下，任何用户都可以从网络访问此计算机，可以根据实际需要撤销某用户或某组从网络访问计算机的权限
拒绝从网络访问这台计算机	如果某些用户只在本地使用，不允许其通过网络访问此计算机，可以将此用户加入本策略
允许在本地登录	此登录权限确定了可交互式登录到该计算机的用户
拒绝本地登录	此安全设置确定阻止哪些用户登录到该计算机，如果一个账户同时受“允许在本地登录”策略制约，则此策略设置将取代“允许在本地登录”策略
关闭系统	加入此策略的用户具有关闭计算机的权限

5.3.3　安全选项

通过本地策略中的安全选项，可以控制一些和操作系统安全相关的设置，安全选项中的策略如图 5-21 所示。

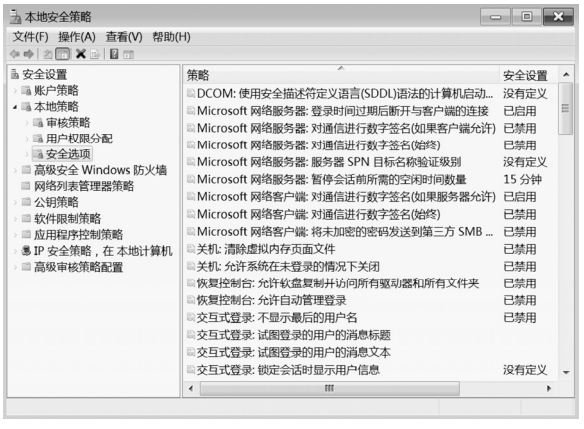


图 5-21　安全选项中的策略

表 5-3 列出了安全选项中的常用安全策略。

表 5-3　安全选项中的常用安全策略

策　略	说　明
关机：允许系统在未登录的情况下关闭	使登录窗口的右下角能够显示关机图标，以便在不需要登录的情况下可以关机
账户：使用空白密码的本地账户只允许进行控制台登录	密码为空的用户不能通过网络访问此计算机，此策略禁用后，密码为空的用户将不会受到限制
交互式登录：用户试图登录时显示的消息文字	指定用户登录时显示的文本消息
交互式登录：用户试图登录时显示的消息标题	用户登录时显示的消息文本窗口标题栏中显示的标题说明

5.3.4　本地组策略

组策略是一组策略的集合，是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具，通过组策略可设置各种软件、计算机和用户策略。在“开始”→“运行”中输入“gpedit.msc”命令，单击“确定”按钮，出现如图 5-22 所示的“本地组策略编辑器”窗口。

图 5-22　“本地组策略编辑器”窗口

本地组策略包含计算机配置和用户配置，各项配置中又分别包含软件设置、Windows 设置和管理模板三部分。计算机配置项的 Windows 设置中的安全设置就是前面介绍的本地安全策略，即本地安全策略是本地组策略的一部分。

ABC 公司文件服务器在插入光盘或 U 盘时，默认情况下会自动播放，此功能虽然给用户带来了很多便利，但也带来了不少麻烦。可以通过设置本地组策略实现禁止自动播放功能。

STEP1　在图 5-22 所示的“本地组策略编辑器”窗口展开“计算机配置”→“管理模板”→“Windows 组件”→“自动播放策略”文件夹，如图 5-23 所示。

STEP2　双击窗口右侧的“关闭自动播放”设置项，弹出“关闭自动播放”窗口，如图 5-24 所示。

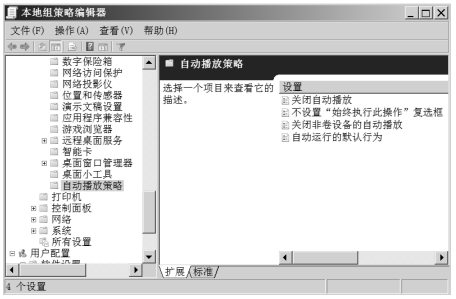


图 5-23　自动播放策略

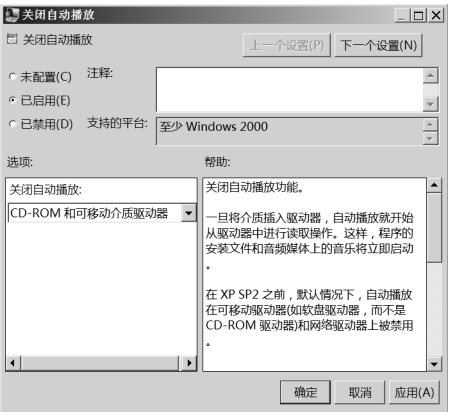


图 5-24　关闭自动播放

STEP3 在“关闭自动播放”窗口选中“已启用”按钮，重启计算机后测试已经关闭了自动播放功能。

5.4　知识介绍——组策略

本地安全策略和本地组策略可以加强工作组中计算机的安全性。组策略适用于在域环境中对多台客户机进行统一配置。通过应用组策略，管理员可以方便地管理 Active Directory 中的用户和计算机的工作环境，如用户桌面环境、计算机启动 / 关机与用户登录 / 注销时所执行的脚本文件、软件安装和安全设置等。

使用组策略，可以实现以下功能。

- 减少布置用户和计算机环境的工作量，只需设置一次，相应的用户或计算机就全部应用设置。
- 减少用户错误配置环境的可能性。
- 可以针对特定对象（用户或计算机）实施特定策略。

5.4.1　组策略结构

组策略的所有配置信息都存放在组策略对象（Group Policy Object，GPO）中，组策略被视为 Active Directory 中的特殊对象，可以将 GPO 和活动目录容器（站点、域、OU）链接起来，以影响容器中的用户和计算机，组策略是通过 GPO 来实现管理的。

1. 默认 GPO

当域创建完成后，默认有两个 GPO，一个是 Default Domain Policy（默认域策略）；另一个是 Default Domain Controller Policy（默认域控制器策略）。选择“开始”→“管理工具”→“组策略管理”，打开“组策略管理”控制台，展开左侧窗格中的各个节点，找到“组策略对象”，打开后可以看到两个默认 GPO，如图 5-25 所示。

注意：

默认的 GPO 不能随意更改，更改后会影响到系统的正常运行。默认的域策略影响域中所有的用户和计算机，默认的域控制器策略影响组织单位“Domain Controllers”中所有的用户和计算机。

图 5-25　默认组策略对象

2．GPO 链接

GPO 用来保存组策略，必须指定 GPO 所链接的对象，才能将组策略应用到指定的对象。GPO 只能链接到 Active Directory 的站点（Site）、域（Domain）或组织单位（Organizational Unit），即活动目录容器，容器中包含的用户和计算机会受到组策略的控制。

单击组策略对象中的“Default Domain Controller Policy”，在右侧窗格中可以看到此 GPO 已经链接到组织单位“Default Controllers”，如图 5-26 所示；单击域“abc.com”下的组策略对象中的 “Default Domain Policy”，在右侧窗格中可看到此 GPO 已经链接到域 abc.com，如图 5-27 所示。

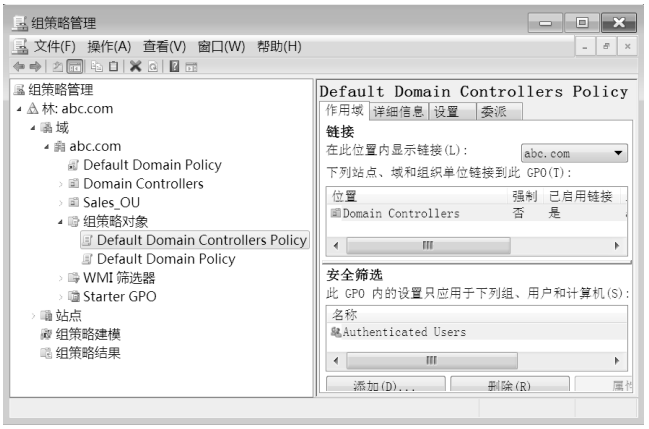


图 5-26　默认域控制器策略

图 5-27　默认域策略

5.4.2　计算机与用户配置

创建组策略的步骤可参考下一节。组策略中包含计算机配置和用户配置，计算机配置对容器中的计算机起作用，用户配置对容器中的用户起作用。

- 计算机配置：计算机配置包括策略和首选项两个部分，如图 5-28 所示。配置这些策略后，容器中所有的计算机都会受其影响。策略中主要包括软件设置、Windows 设置和管理模板 3 部分。

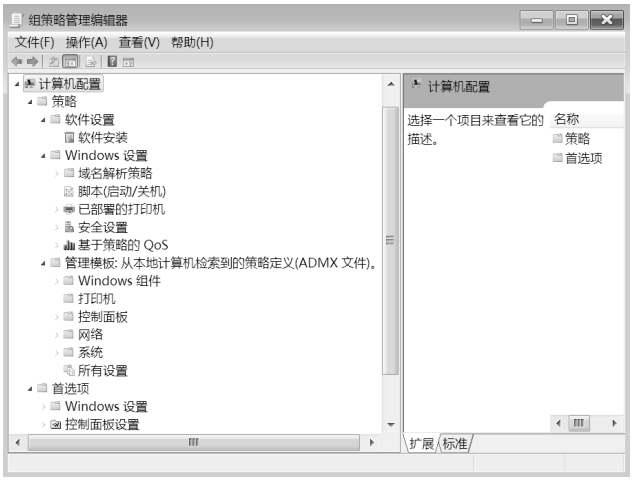


图 5-28　计算机配置

- 用户配置：用户配置包括策略和首选项两个部分，如图 5-29 所示。配置这些策略后，容器中所有的用户都会受其影响，用户配置策略与计算机配置策略包括的内容相似。

注意：

计算机配置一般需要重新启动后计算机才能生效，用户配置一般是用户重新登录就可以生效。

图 5-29　用户配置

5.5　任务 3：组策略的简单应用

5.5.1　组策略应用实例

ABC 公司的网络是域结构，销售部员工的用户账户位于 Sales_OU 中，现要求销售部的员工禁止运行 Internet Explorer，通过以下步骤能够实现上述要求。

STEP1 利用域管理员账号登录 DC，选择“开始”→“管理工具”→“组策略管理”，打开组策略管理页面。右键单击“Sales_OU”，选择“在这个域中创建 GPO 并在此处链接”，如图 5-30 所示。

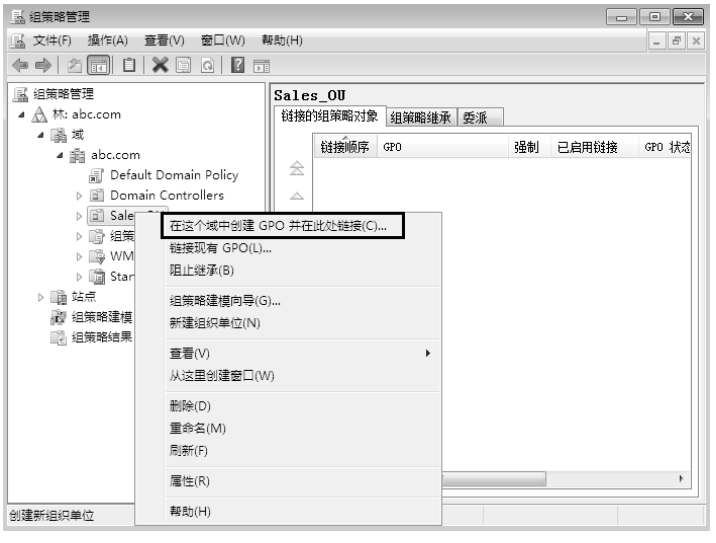


图 5-30　创建并链接 GPO

STEP2 在“新建 GPO”对话框中输入 GPO 的名字为“销售部 GPO”，单击“确定”按钮，如图 5-31 所示。

图 5-31　新建 GPO

STEP3 右键单击“销售部 GPO”，选择“编辑”，打开“组策略管理编辑器”窗口，展开“用户配置”→“策略”→“管理模板”→“系统”，在右侧众多选项中找到“不要运行指定的 Windows 应用程序”，如图 5-32 所示。

图 5-32　组策略管理编辑器

STEP4 双击 “不要运行指定的 Windows 应用程序”，打开“不要运行指定的 Windows 应用程序”窗口，选择“已启用”，如图 5-33 所示。

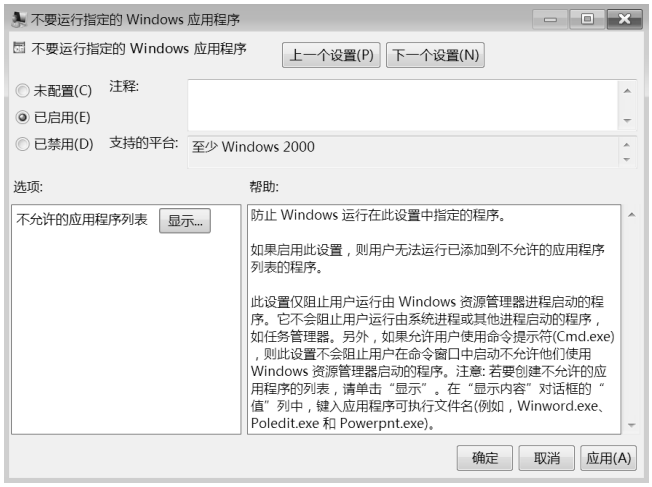


图 5-33 “不要运行指定的 Windows 应用程序”窗口

STEP5 单击图 5-33 中的“显示”按钮，在如图 5-34 所示的“显示内容”对话框的“值”列中，键入 Internet Explorer 应用程序可执行文件名 iexplore.exe，单击“确定”按钮。

图 5-34 “显示内容”对话框

STEP6 以 Sales_OU 中的用户 UserA 账户在域内的客户机登录，运行 Internet Explorer 浏览器，但已被禁止运行，如图 5-35 所示。

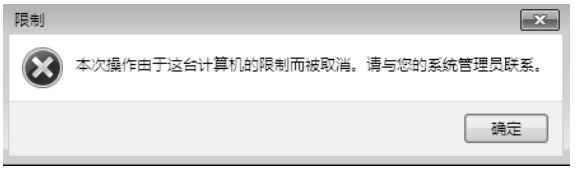


图 5-35　禁止运行 Internet Explorer

注意：

如果其他部门的 OU 要应用与 Sales_OU 同样的组策略设置，不需要在该部门 OU 创建新的 GPO，可以利用 GPO 的链接来实现。右键单击其他部门 OU，选择“链接现有 GPO”，在“选择 GPO”对话框中单击要链接的 GPO，然后单击“确定”按钮。

ABC 公司希望所有用户在域中的计算机上登录时，能够显示信息，让用户在登录前阅读公司计算机使用规范。通过以下步骤能够实现上述要求。

STEP1 选择“开始”→“管理工具”→“组策略管理”，打开组策略管理页面。右键单击“abc.com”，选择 “在这个域中创建 GPO 并在此处链接”，在“新建 GPO”对话框中输入 GPO 的名字为“Domain Policy1”，单击“确定”按钮。

STEP2 右键单击“Domain Policy1”，选择“编辑”，打开“组策略管理编辑器”窗口，展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”，双击右侧的“交互式登录：试图登录的用户的消息标题”，选择“定义此策略设置”，在 5-36 所示的文本框中输入“注意”，依次单击“应用”和“确定”按钮。

STEP3 双击“交互式登录：试图登录的用户的消息文本”，选择“在模板中定义此策略设置”，在下面的文本框中输入内容，依次单击“应用”和“确定”按钮，如图 5-37 所示。

STEP4 启动加入域内的计算机，登录前会显示如图 5-38 所示的界面：用户登录时显示的消息。

图 5-36　试图登录用户的消息标题

图 5-37　试图登录用户的消息文本

图 5-38　用户登录时显示的消息

5.5.2　组策略应用规则

组策略可以影响域内所有用户或计算机，在应用组策略前要明确组策略的应用规则，如组策略继承、累加、应用顺序和强制继承等，以方便利用这些规则实现用户的需求。

1．继承、阻止继承和强制继承

在默认情况下，下层容器会继承来自上层容器的 GPO，如在图 5-39 中，组织单位 Sales_Ou 会继承域 abc.com 的组策略，组织单位 gd_sales 会继承上级组织单位 Sales_Ou 的组策略。

子容器可以阻止继承上层容器的组策略，在图 5-39 中，若要配置组织单位 gd_sales 阻止继承上级 OU 的策略，可以右键单击 gd_sales，选择“阻止继承”。还可以右键单击 Sales_Ou

的 GPO（销售部 GPO），选择“强制”，表示下级子容器必须继承此 GPO 的策略，无论下级子容器是否选择阻止继承。

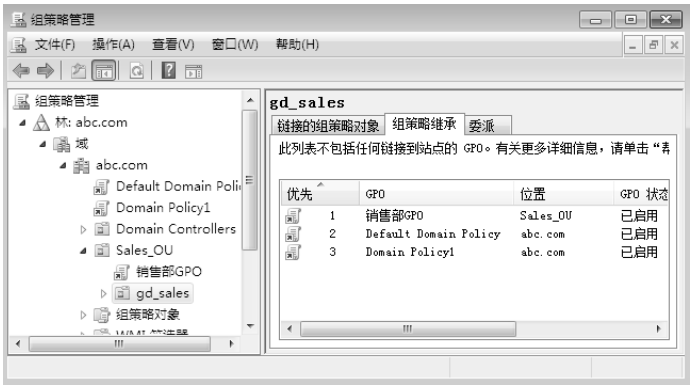


图 5-39　组策略的继承

2．累加

如果容器的多个组策略设置不冲突，则最终的有效策略是所有组策略设置的累加。例如，将域 abc.com 链接到组策略对象 a，将组织单位 Sales_Ou 链接到组策略对象 b，则组织单位 Sales_Ou 会同时应用 a 和 b 这两个组策略对象。

如果容器的多个组策略设置冲突，即对相同项目进行了不同的设置，在默认情况下，后应用的组策略将覆盖先应用的组策略。例如，域的组策略设置禁止用户运行 Internet Explorer，OU 的组策略设置可以运行，则在默认情况下，OU 的有效设置是可以运行 Internet Explorer。

3．应用顺序

组策略按以下顺序应用：本地策略、站点策略、域策略和组织单位策略。在默认情况下，当策略设置发生冲突时，后应用的策略将覆盖前面的策略。

每台计算机都只有一个本地组策略对象（“开始”→“管理工具”→“本地安全策略”）。如果计算机在工作组环境下，将应用本地组策略；如果计算机加入域，则除了受到本地组策略的影响，还可能受到站点、域和 OU 的组策略影响；如果策略之间发生冲突，则后应用的策略起作用。总之，组策略应用顺序如下所述。

- 首先应用本地组策略对象。
- 如果有站点组策略对象，则应用。
- 然后应用域组策略对象。
- 如果计算机或用户属于某个 OU，则应用 OU 上的组策略对象。
- 如果计算机或用户属于某个 OU 的子 OU，则应用子 OU 上的组策略对象。
- 如果同一个容器下链接了多个组策略对象，则按照链接顺序从大到小逐个应用。

5.5.3　组策略的筛选

上面介绍的 GPO 都是应用于容器下的所有用户和计算机，但在实际环境中会有这样的

需求。例如，销售部的所有普通用户都受 GPO 约束，而销售部经理的账户不受此约束，使用组策略的筛选可以实现。筛选可以阻止一个 GPO 应用于容器内部的特定用户和计算机。

容器中的用户和计算机之所以受到 GPO 影响，是因为他们对 GPO 拥有读取和应用组策略的权限。如果用户或计算机账户没有读取和应用组策略的权限，组策略将拒绝执行。

假设上例中 Sales_Ou 中的 UserA 账户是经理，UserB 账户为普通用户，希望 UserA 登录后可以运行 Internet Explorer 应用程序，可以通过以下步骤完成。

STEP1 在“组策略管理”页面，单击“销售部 GPO”，在右侧窗口中单击“委派”标签，如图 5-40 所示。

STEP2 单击“高级”按钮，出现“销售部 GPO 安全设置”对话框，添加 UserA 账户拒绝读取和拒绝应用组策略权限，如图 5-41 所示。

STEP3 分别以 UserA 和 UserB 账户登录域，验证组策略设置效果。UserA 账户可以运行 Internet Explorer，而 UserB 账户被拒绝。

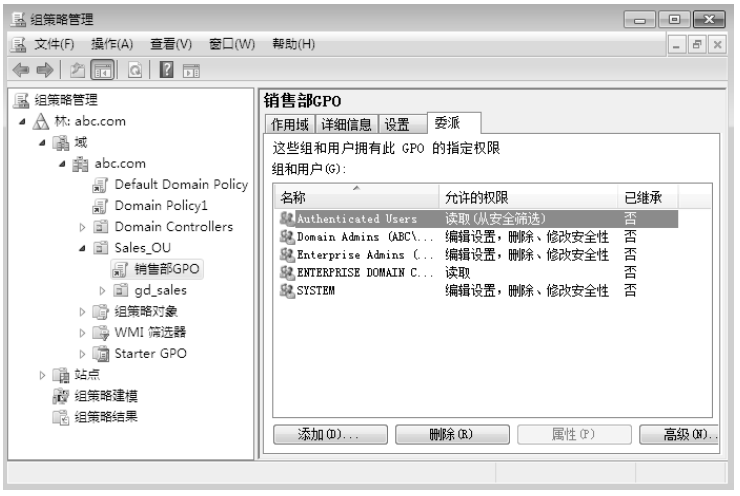


图 5-40　销售部 GPO 的委派标签

图 5-41　拒绝权限

5.6　任务 4：利用组策略实现软件分发

网络管理员在布置域中的软件时，经常会在域中多台计算机上安装、修复、卸载和升级同一软件。如果在每台计算机上重复这些操作，工作量大而且容易出错。利用 GPO 设置软件分发策略，可以实现对容器中所有用户和计算机的软件管理。

1．分发软件

利用 GPO 给容器中的计算机或者用户分发软件，需要以下几个步骤。

- 准备安装程序包文件，该程序包包含一个.msi 文件以及必要的相关安装文件。
- 将安装程序包文件存放到服务器上的一个共享文件夹内。
- 创建或编辑分发软件的 GPO。

ABC 公司销售部的所有用户都需要使用 Office 办公软件，希望销售部用户登录时能自动安装该软件。

STEP1　在服务器上建立名为 software 的文件夹，将 Microsoft Office 2003 CD 内的安装文件复制到 software 文件夹内，并将文件夹共享，赋予 Everyone 读取权限。

STEP2　在“组策略管理”页面，右键单击“Sales_Ou”，选择“在这个域中创建 GPO 并在此处链接”，输入新建 GPO 的名称“Soft_Policy”。右键单击“Soft_Policy”，选择“编辑”，依次展开“用户配置”→“策略”→“软件设置”，右键单击“软件安装”，选择“属性”，如图 5-42 所示。

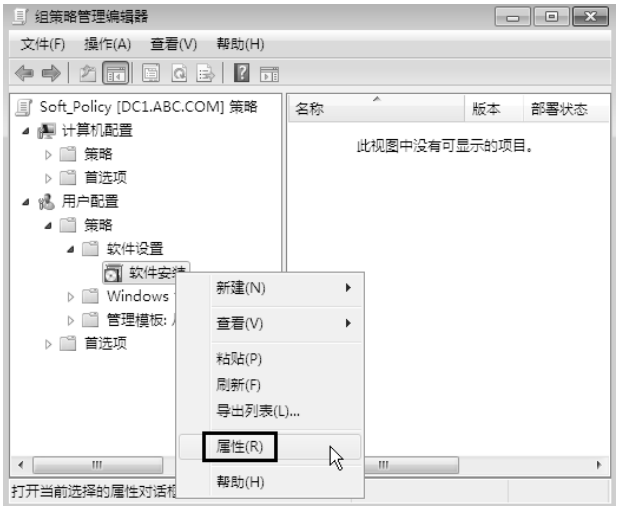


图 5-42　软件安装属性

STEP3　在图 5-43 所示的“默认程序数据包位置”文本框中输入软件的存储位置，即安装程序包文件所在的共享文件夹 UNC 路径，例如，\\192.168.1.1\software，完成后单击“确定”按钮。

图 5-43　软件安装属性

STEP4 右键单击“软件安装”，选择“新建”→“数据包”，如图 5-44 所示，指定默认程序数据包位置。

图 5-44　默认程序数据包位置

STEP5 在如图 5-45 所示的页面选择 Microsoft Office 2003 安装文件 PRO11.MSI，单击“打开”按钮，新建数据包。

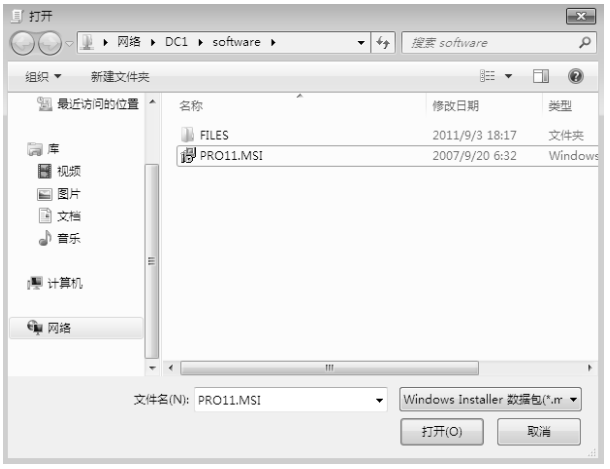


图 5-45　新建数据包

STEP6 在如图 5-46 所示的“部署软件”页面中将选择部署方法设置为“已分配”，单击“确定”按钮，显示软件分配状态为已分配，如图 5-47 所示。

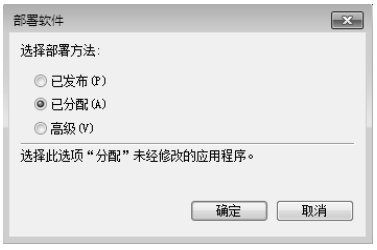


图 5-46　选择部署方法

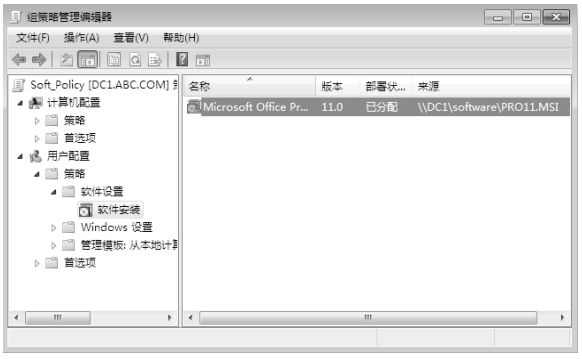


图 5-47　软件分配状态

STEP7 右键单击图 5-47 中已发布的软件包，选择“属性”，在“部署”选项卡中设置“在登录时安装此应用程序”，单击“应用”按钮，如图 5-48 所示。

STEP8 利用 Sales_OU 中的用户 UserA 在加域的客户机上登录，进入系统后，会发现桌面上已经安装了 Microsoft Office 2003 组件的快捷方式，当用户第一次使用这些软件时，系统会安装这些功能，如图 5-49 所示。

图 5-48　设置部署选项

图 5-49　客户机上安装的软件

注意:

分配与发布有区别，分配可以将程序分配到用户或计算机，当用户登录到计算机时就会安装此程序，用户第一次运行此程序时，安装过程最终完成；分配具有强制性。发布只可以将程序发布给用户，不可以发布给计算机，当用户登录到计算机时，发布的程序显示在“控制面板”的“程序”中，要想使用软件需要进一步安装完成；发布具有可选性。

2．修复软件

管理员利用 GPO 不但可以方便地为域中的用户和计算机分发软件，还可以方便地修复软件，如果用户的软件发生丢失或损坏，客户端系统会自动检测到这一错误，并重新安装这些文件。

如果原软件分发点上的安装文件也发生丢失或损坏，则必须先到服务器上修复源文件，再将其重新部署。在组策略编辑器中右键单击分发的程序包，如图 5-50 所示，选择“所有任务”→“重新部署应用程序”，弹出询问对话框，单击“是”按钮，则强制所有安装此软件的客户端重新再安装一次。

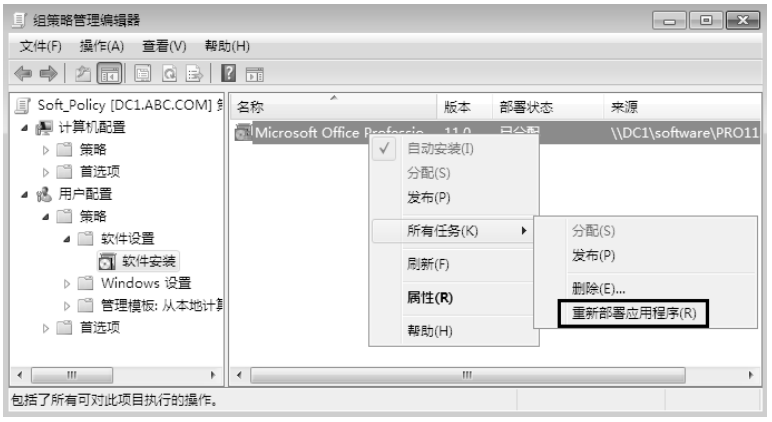


图 5-50　重新部署应用程序

3．删除软件

当用户或者计算机不再需要分发的软件时，可以在 GPO 中删除软件，右键单击要删除的程序包，在如图 5-50 所示的页面中，选择“删除”，弹出“删除软件”对话框，选择删除方法，如图 5-51 所示。

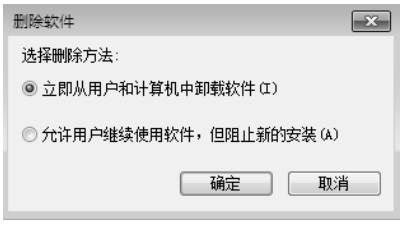


图 5-51　删除软件

5.7　实训

实训环境一

HT 公司有一台 Windows Server 2008 服务器位于工作组中，为了加强该服务器的安全性，需要配置密码策略和账户锁定策略，账户被锁定后，只有管理员账户才能解锁。文件服务器

上有一个文件夹 D:\data，为了加强数据的安全性，管理员需要审核所有用户账户对该文件夹的访问情况。

需求描述

- 启用密码复杂性策略，配置密码最短长度要求。
- 配置账户锁定阈值。
- 启用审核对象访问策略。
- 查看审核结果。

实训环境二

HT 公司搭建了 Windows Server 2008 域，域中有多个用户账户，域中所有用户要使用统一桌面背景，不能使用 Internet Explorer 浏览器，部门经理除外。域中所有计算机开机显示“使用计算机须知”。域内所有用户要使用 Office 2007，用最快办法为域中的用户安装此软件。

需求描述

- 在域上创建并链接一个组策略。
- 对组策略进行配置，统一域用户的桌面背景，不能运行 Internet Explorer 程序。
- 对组策略进行配置，设置用户登录时显示的消息标题和消息文字。
- 建立软件分发站点并共享，准备好 Office 2007 安装包。
- 通过配置组策略将 Office 2007 分发给所有域用户。

5.8　习题

- 在本地安全策略中，密码策略主要包含哪些具体策略？
- 在本地安全策略中，账户锁定策略主要包含哪些策略？
- 组策略能应用到哪些容器对象？
- 组策略的应用顺序是什么？
- 组策略的计算机配置与用户配置作用有什么不同？
- 应用组策略发布软件与分配软件有什么区别？

第6章

磁盘管理

项目需求：

ABC 公司的文件服务器存储的内容越来越多，需要增加磁盘空间。该服务器原有一块 SCSI 硬盘，并且安装了 Windows Server 2008 R2 操作系统，要增加 3 块 SCSI 硬盘，用来存放数据。要求有良好的读写速度，一定的容错功能，较高的空间利用率。文件服务器上的驱动器 F：是为用户存储文件的，要求限制普通用户使用磁盘空间。

技能目标：

- 了解磁盘分区方式、类型
- 会配置基本磁盘
- 理解动态磁盘
- 会配置简单卷、跨区卷、带区卷、镜像卷和 RAID-5 卷
- 会使用磁盘配额限制用户使用磁盘空间

MEMO

6.1 知识介绍——磁盘管理概述

磁盘是计算机的重要存储设备，所有的磁盘在使用前都必须经过初始化，在进行磁盘初始化时，要选择磁盘分区形式。

1．MBR 分区

MBR（Master Boot Record，主引导记录）第一个扇区内保存着引导程序和硬盘分区表，共计 64 字节，分区表中存储着硬盘每个分区的信息，包括起始柱面号和结束柱面号，每个分区信息占 16 字节，一共可容纳 4 个主分区信息，所以每块硬盘最多划分四个分区。为了划分更多分区，可以对某一分区进行扩展，在扩展分区上再次划分逻辑分区。

2．GPT 分区

GPT（GUID Partition Table，GUID 分区表）突破了 64 字节的固定大小限制，支持每个磁盘上多于四个分区，在 Windows Server 2008 R2 系统下最多可划分 128 个主区。

Windows Server 2008 R2 提供了强大的磁盘管理工具对磁盘进行管理、优化并维护。选择“开始”→“管理工具”→“计算机管理”，在“计算机管理”窗口左侧选择“存储”→“磁盘管理”，显示磁盘管理工具窗口，如图 6-1 所示。利用磁盘管理工具可以控制磁盘联机或脱机，以及创建卷等。

图 6-1 磁盘管理

6.1.1 磁盘类型

Windows Server 2008 R2 依据磁盘的配置方式，将磁盘分为两种类型：基本磁盘和动态磁盘。

1．基本磁盘

基本磁盘是一种包含主磁盘分区、扩展磁盘分区或逻辑分区的物理磁盘，基本磁盘上的分区称为基本卷，只能在基本磁盘上创建基本卷，可以向现有分区添加更多空间，但仅限于同一物理磁盘上的连续未分配的空间。如果要跨磁盘扩展空间，需要使用动态磁盘。

2．动态磁盘

动态磁盘打破了分区只能使用连续的磁盘空间的限制，扩展分区可以灵活地使用多块硬盘上的空间。使用动态磁盘可获得更高的可扩展性、读写性能和可靠性。

6.1.2　磁盘分区

在使用基本磁盘方式管理磁盘时，首先要将磁盘划分为一个或多个磁盘分区，才可以向磁盘中存储数据。以下磁盘分区以 MBR 类型分区为例。

1．主分区

主分区是可以用来引导操作系统的分区，一般就是操作系统的引导文件所在的分区。在 Windows Server 2008 R2 中，每块基本磁盘的前 3 个分区都将自动创建为主分区，每块基本磁盘最多可以创建 4 个主分区或者 3 个主分区加上一个扩展分区。每个主分区都可以引导磁盘上的操作系统，但同时只能有一个主分区处于激活状态。

多个主分区的优点是可以互不干扰地安装多个操作系统，用户可通过激活不同的主分区而引导不同的操作系统。当某一个主分区的操作系统损坏时，不会影响到在其他主分区上安装的操作系统。磁盘四种主分区的分区结构如图 6-2 所示。

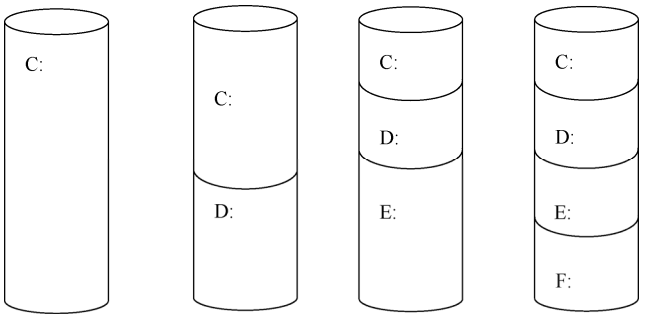


图 6-2　磁盘四种主分区的分区结构

2．扩展分区

如果主分区的数量达到 3 个，磁盘上还有未分配的磁盘空间，执行“新建简单卷”就会将剩余的空间划分为扩展分区空间使用，每一块硬盘上只能有一个扩展分区。扩展分区不能用来启动操作系统，并且扩展分区在划分之后不能直接使用，不能被赋予盘符，必须要在扩展分区中划分逻辑分区才可以使用。

一个扩展分区可以划分成多个逻辑分区。扩展分区的结构如图 6-3 所示。

3．逻辑分区

用户不能直接访问扩展分区，而是需要在扩展分区内部再划分若干个部分，称为逻辑分区。每个逻辑分区都可以被赋予一个盘符。逻辑分区不能直接用来启动操作系统，但可以将操作系统的引导文件放到主分区上，而将操作系统的其他文件存放到逻辑分区上。

在 Windows Server 2008 R2 中，如果所需分区的数量小于等于 3，则创建的分区都是主分区，如果分区的数量大于 3，则将创建 3 个主分区和一个扩展分区，然后在扩展分区中建立若干个逻辑分区。

逻辑分区的分布结构如图 6-4 所示。

图 6-3　扩展分区的结构

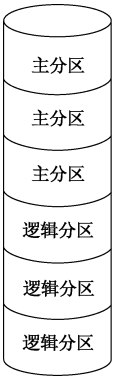


图 6-4　逻辑分区的分布结构

6.2　任务 1：基本磁盘管理

在图 6-1 所示的磁盘管理工具中显示的“磁盘 0”为基本磁盘，此磁盘在安装 Windows Server 2008 R2 时就被划分为图中的两个分区，其中第一个为系统保留区域，容量约 100 MB，此分区为系统卷和启动卷，没有驱动器号；另一个磁盘分区的驱动器号为（C:），是安装了 Windows Server 2008 R2 的启动卷。

在计算机内安装新磁盘后，必须经过初始化后才可以创建分区并使用。选择“开始”→“管理工具”→“计算机管理”→“存储”→“磁盘管理”，会自动弹出如图 6-5 所示的“初始化磁盘”对话框。如果未自动弹出此对话框，右键单击新磁盘，选择“联机”，如图 6-6 所示。联机后再右键单击该磁盘，选择“初始化磁盘”。

图 6-5　初始化磁盘

注意：

在进行初始化磁盘时，如果对话框中看不到新磁盘，则选择磁盘管理工具窗口的菜单项“操作”→“重新扫描磁盘”。

图 6-6　联机磁盘

6.2.1　创建主分区

在一个基本磁盘（如磁盘 1）上创建主分区的步骤如下所述。

STEP1　在图 6-1 所示的“磁盘管理”工具中右键单击磁盘 1，选择“新建简单卷”，如图 6-7 所示。

图 6-7　新建简单卷

STEP2　在“欢迎使用新建简单卷向导”页面中单击“下一步”按钮。在“指定卷大小”页面中输入主分区的大小，如图 6-8 所示，单击“下一步”按钮。

STEP3　在“分配驱动器号和路径”页面中选择一个未使用的驱动器号，如图 6-9 所示，然后单击“下一步”按钮。

STEP4　在“格式化分区”页面中设置格式化选项，如图 6-10 所示，单击“下一步”按钮。

图 6-8　指定卷大小

图 6-9　分配驱动器号和路径

图 6-10　格式化分区

STEP5 在“正在完成新建简单卷向导”页面中确认已选择的设置，单击“完成”按钮。系统将完成磁盘格式化操作，创建完成的主分区（F:）如图 6-11 所示。

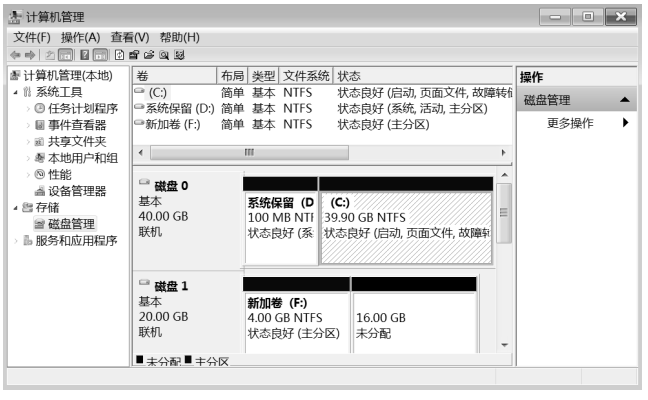


图 6-11　创建完成的主分区（F:）

6.2.2　创建扩展分区

Windows Server 2008 R2 不提供图形界面创建扩展分区，需要使用 diskpart.exe 程序。例

如在图 6-11 中的 16 GB 未分配空间创建一个 10 GB 的扩展分区，在命令提示行输入 diskpart 命令，再输入 select disk 命令选择要创建扩展分区的磁盘，输入 creat partition extended size=10240 命令创建 10 GB 扩展分区（默认为 MB）。创建完成后，执行 exit 命令退出分区命令，如图 6-12 所示。

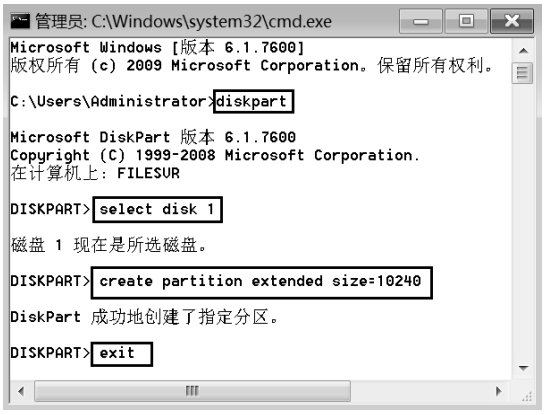


图 6-12　创建扩展分区

6.2.3　创建逻辑分区

一个扩展分区内可以创建多个逻辑分区，在“磁盘管理”工具中右键单击扩展分区（绿色区域），选择“新建简单卷”，后续步骤与创建主分区的操作基本相同，创建的逻辑分区（G:）如图 6-13 所示。

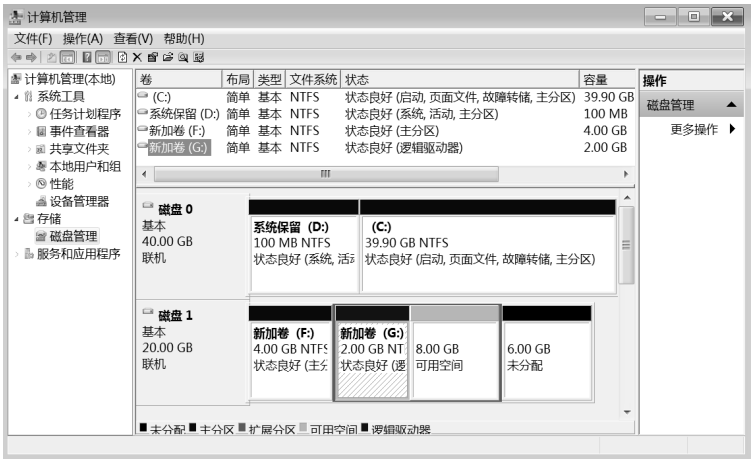


图 6-13　创建的逻辑分区（G:）

6.2.4　删除分区

要删除主分区，只需右键单击要删除的分区，选择“删除卷”命令，按提示完成即可。要删除扩展分区，必须首先删除其中的逻辑分区（方法与删除主分区的方法基本相同），再

右键单击扩展分区，选择“删除分区”命令，按提示完成相应操作。

6.3 任务 2：动态磁盘管理

要使磁盘具有较强的扩展性和可靠性（具有容错功能）等特性，就需要将基本磁盘转换成动态磁盘。Windows Server 2008 R2 支持的动态磁盘卷有 5 种类型：简单卷、跨区卷、带区卷、镜像卷和 RAID-5 卷，使用磁盘管理工具可以管理各种类型的动态磁盘卷。

ABC 公司的文件服务器增加了 3 块 SCSI 硬盘用于存储重要数据，要求有良好的读写速度和一定的容错功能，并具有较高的空间利用率，在 5 种动态卷类型中选择合适的卷来管理。

6.3.1 基本磁盘和动态磁盘的转换

Windows Server 2008 R2 系统默认使用的磁盘类型是基本磁盘，要将指定的磁盘由基本磁盘转换成动态磁盘，可以使用磁盘管理工具实现。

由基本磁盘转化成动态磁盘，需要注意以下问题。

- 如果磁盘包括当前的操作系统或者引导文件，则转换需要重启后才能完成。
- 当基本磁盘转换为动态磁盘后，所有的磁盘分区将变成简单卷。
- 在转换磁盘之前，必须先关闭该磁盘运行的所有程序。

右键单击需要转换的基本磁盘，选择“转换到动态磁盘”，如图 6-14 所示。

图 6-14 转换到动态磁盘（1）

在“转换为动态磁盘”对话框中，列出了本地计算机中所有可用的基本磁盘，选择要转换的（一个或多个）基本磁盘，如图 6-15 所示。

进一步确认要转换的基本磁盘，可以查看要转换的基本磁盘的详细信息（如分区情况）。最后系统会弹出一个信息框，提示基本磁盘一旦转换为动态磁盘，将无法从这些磁盘的卷启动已安装的操作系统。完成转换后，在磁盘管理窗口中可以看到原来的基本磁盘已经转换成动态磁盘，而原来所有的分区都转换成了简单卷，如图 6-16 所示。

图 6-15　转换到动态磁盘（2）

图 6-16　转换后的动态磁盘和卷

将基本磁盘转换为动态磁盘之后，便可以在其中创建动态磁盘卷了。如果系统中有多块磁盘，由于 Windows Server 2008 R2 允许基本磁盘和动态磁盘共存，所以，可以将部分或全部的磁盘转换成动态磁盘，也可以保留基本磁盘。当将动态磁盘上的所有卷都删除后，动态磁盘将自动转换成基本磁盘。

6.3.2　简单卷

简单卷是动态卷中的基本单元，它的地位与基本磁盘中的主分区相当。可以从一个动态磁盘内选择未分配空间来创建简单卷，并且在必要的时候可以将简单卷扩展。如果跨多个磁盘扩展简单卷，则该卷将变为跨区卷。简单卷不能容错，但可以随时添加镜像，从而将简单卷转换为镜像卷。

在磁盘管理工具中右键单击动态磁盘的空闲空间，选择“新建简单卷”，如图 6-17 所示。在“欢迎使用新建简单卷向导”页面中单击“下一步”按钮，接下来指定卷的大小及分配驱动器号，选择格式化文件系统并执行格式化操作。

当简单卷的空间需要扩展时，可将空闲空间合并到简单卷。只有尚未格式化或已被格式化为 NTFS 的卷才可以被扩展。在磁盘管理工具中右键单击要扩展的简单卷，选择“扩展卷”，如图 6-18 所示。在扩展卷向导中选择扩展的磁盘及空间大小，如图 6-19 所示，按照提示完成简单卷的扩展。

图 6-17　新建简单卷

图 6-18　扩展卷

图 6-19　选择磁盘

6.3.3　跨区卷

跨区卷可以将分散在多个硬盘（2～32 个）上的硬盘空间组合在一起，形成一个较大的

存储空间，每块硬盘所提供的磁盘空间不必相同，用户在使用时不会感觉到在使用多个硬盘。在磁盘管理工具中右键单击未分配的区域，选择“新建跨区卷”，依据向导的提示，选择磁盘和空间，如图 6-20 所示，图中磁盘 1 提供 4 GB 的空间，磁盘 2 提供 10 GB 的空间，跨区卷的容量就是 14 GB，接下来指定驱动器号并格式化分区，完成跨区卷（G:）的创建，如图 6-21 所示。虽然利用跨区卷可以快速增加卷的容量，但它既不能提高对磁盘数据的读写性能，也不具有任何容错功能。

图 6-20　选择跨区卷的磁盘和空间

图 6-21　跨区卷（G:）

6.3.4　带区卷

带区卷也叫条带卷或 RAID-0 卷，它由两块或两块以上（2～32 个）硬盘组成，每块硬盘所提供的磁盘空间大小必须相同。带区卷上的数据被均匀地以数据块的形式跨磁盘交替分配，带区卷是所有卷中运行效率最好的卷。

在磁盘管理工具中右键单击未分配的区域，选择“新建带区卷”，依据向导的提示，选择磁盘和空间，如图 6-22 所示，图中磁盘 1、2 提供相同的 4 GB 空间，带区卷的容量为 4 GB×2，即 8 GB。接下来指定驱动器号并格式化分区，完成带区卷（H:）的创建，如图 6-23 所示。

图 6-22　选择带区卷的磁盘和空间

图 6-23　使用两块硬盘建立的带区卷（H:）

6.3.5　镜像卷

镜像卷是在两个物理磁盘上复制数据的容错卷，又叫 RAID-1 卷。每个硬盘提供相大小同空间，镜像卷提供了数据冗余以复制卷上包含的信息。镜像总是位于另一个磁盘上，如果其中一个物理磁盘出现故障，则该故障磁盘上的数据将不可用，但系统可以在位于另一个磁盘上的镜像中继续进行操作。镜像卷的容量是组成镜像卷的所有磁盘空间和的一半。

在磁盘管理工具中右键单击动态磁盘的空闲空间，选择“新建镜像卷”。按照“欢迎使用镜像卷向导”提示，选择磁盘和空间，如图 6-24 所示，接下来指定驱动器号并格式化分区，完成镜像卷的创建，如图 6-25 所示镜像卷（I:），它的实际容量为 2×2 GB/2 即 2 GB。

当不需要镜像卷的时候可以像删除磁盘分区一样，将镜像卷删除，镜像卷上面存储的数据也会一同丢失。如果中断镜像，会将镜像卷分解成两个简单卷，上面存储的数据不会受到影响。可以在镜像卷中的一块磁盘损坏的时候中断镜像，然后替换损坏的硬盘，最后为镜像卷中没有损坏的磁盘添加镜像，即可恢复损坏的镜像卷。

图 6-24　选择镜像卷的磁盘和空间

图 6-25　镜像卷（I:）

6.3.6　RAID-5 卷

RAID（Redundant Array of Inexpensive Disks，廉价冗余磁盘阵列）简称为磁盘阵列。可以把 RAID 理解成一种使用磁盘驱动器的方法，它将一组磁盘驱动器用某种逻辑方式联系起来，作为逻辑上的一个磁盘驱动器来使用。

RAID-5 卷是具有容错功能的磁盘阵列，它至少需使用 3 块硬盘才能建立，每块硬盘必须提供相同的磁盘空间。在使用 RAID-5 卷时，数据除了会分散写入各硬盘中，还会同时建立一份奇偶校验数据信息，保存在不同的硬盘上。若有一块硬盘发生故障，可由剩余的磁盘数据结合校验信息计算出该硬盘上原有的数据。RAID-5 卷的磁盘空间利用率为（n–1）/n×100%（n 为磁盘数），与镜像卷相比，有较高的磁盘利用率。

在磁盘管理工具中右键单击动态磁盘的空闲空间，选择“新建 RAID-5 卷”。按照“欢迎使用镜像卷向导”提示，选择磁盘和空间，如图 6-26 所示，接下来指定驱动器号并格式化分区，完成 RAID-5 卷的创建，如图 6-27 所示 RAID-5 卷（J:）。

RAID 的实现方式有软件和硬件两种。硬件方式使用专门的硬件设备，如 RAID 卡和 SCSI 硬盘等。由于使用软件实现磁盘阵列，其性能优势并不明显。在实际中一般采用硬件实现磁盘阵列。

图 6-26　选择 RAID-5 卷的磁盘和空间

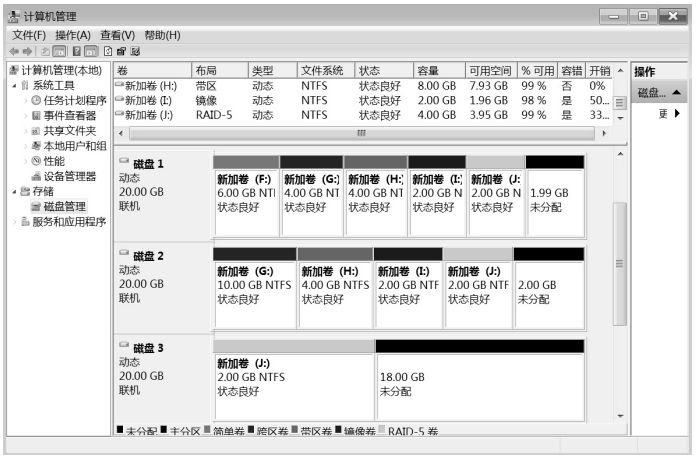


图 6-27　RAID-5 卷（J:）

6.4　任务 3：使用磁盘配额

利用磁盘配额功能可以限制用户使用磁盘空间。当用户存储的文件达到指定的容量时，将会出现磁盘空间已满的提示。磁盘配额能够避免因某个用户的过度使用磁盘空间造成其他用户无法正常工作甚至影响系统运行的情况发生，避免发生由于磁盘空间使用失控可能造成的系统崩溃，提高了系统的安全性。

磁盘配额限制用户账户使用卷（或分区）的磁盘空间，每个用户账户对磁盘空间的利用都不会影响同一卷上的其他用户账户的磁盘配额。例如，如果卷（F:）的配额限制是 500 MB，某用户已在卷（F:）中保存了 500 MB 的文件，此时即便卷（F:）中仍有空闲空间，该用户也必须首先删除一些现有文件之后才可以将其他数据写入该卷中。只要有足够的空间，其他每个用户就可以在该卷中保存最多 500 MB 的文件。

当启用磁盘配额后，除了 Administrators 组的成员，其他所有用户账户都将受到配额的限制。

ABC 公司文件服务器的卷（E:）中有一个共享的文件夹 home，供域用户存储文件，网

络管理员发现个别员工在其中存放了大量与工作无关的文件，导致卷（E:）空间消耗量很大，他希望限制用户可以使用的磁盘空间。普通员工限制为 100 MB，超过 90 MB 就记录警告信息，部门经理 Manager1 限制为 200 MB，超过 180 MB 就记录警告信息，步骤如下。

STEP1 右键单击卷（E:），选择“属性”，打开属性对话框中 “配额”标签，选择“启用配额管理”，选择“拒绝将磁盘空间给超过配额限制的用户”，将磁盘空间限制为 100 MB，将警告等级设为 90 MB。再选择“用户超出配额限制时记录事件”和“用户超过警告等级时记录事件”，如图 6-28 所示，单击“确定”按钮。

STEP2 单击如图 6-28 所示的“配额项”按钮，在工具栏中选择“配额”→“新建配额项”，选择域账户 Manager1 后，配置磁盘空间限制，如图 6-29 所示，单击“确定”按钮。

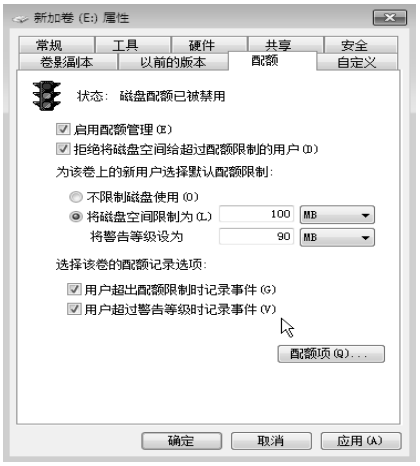


图 6-28　启用配额管理

图 6-29　配额设置对话框

STEP3 设置完成后，使用普通用户账户向（E:）中写入文件，如果达到 100 MB，将收到空间不足的信息，如图 6-30 所示。管理员可以使用“事件查看器”跟踪用户使用磁盘空间的情况。

图 6-30　新加卷（E:）上空间不足

磁盘配额可以限制指定账户能够使用的磁盘空间，这样可以避免发生因某个用户过度使用磁盘空间造成其他用户无法正常工作甚至影响系统的运行情况。在服务器管理中此功能非常重要，但对单机用户来说意义不大。

6.5 实训

实训环境

HT 公司为文件服务器增加了 3 块 500 GB 硬盘，为了方便使用，创建简单卷用来存放各部门的技术资料，建立 RAID-5 卷用来存放财务部的重要资料。限制各部门存储资料使用的磁盘空间大小，部门经理为 500 MB，普通员工为 200 MB。

需求描述

- 安装硬盘并初始化。
- 将新添加的基本磁盘转换为动态磁盘。
- 在磁盘 1 上创建一个大小为 80 GB 的简单卷。
- 对简单卷进行扩展，使其容量增大为 90 GB。
- 将简单卷扩展到磁盘 2，使其容量为 100 GB（变为跨区卷）。
- 利用三块硬盘剩余的空间创建 RAID-5 卷。
- 为简单卷启用磁盘配额。

6.6 习题

- MBR 分区与 GPT 分区相比较有哪些不同？
- 使用动态磁盘与使用基本磁盘相比有哪些优势？
- Windows Server 2008 R2 支持的动态磁盘卷类型有哪些？
- 在 Windows Server 2008 R2 支持的动态磁盘卷中，哪些卷具有容错功能？

第 7 章

配置 DHCP 服务

项目需求：

ABC 公司原来的局域网规模很小，以手动的方式为局域网内的计算机配置 IP 地址。随着公司计算机数量的增多，工作量加大，管理员手工为员工设置 IP 地址，经常出现“IP 地址冲突”现象，需要将计算机设置为自动获取 IP 地址、网关、首选 DNS 服务器等参数。为保证用户能够正常连接到打印服务器，需要使该服务器始终获得同一个 IP 地址。

技能目标：

- 理解 DHCP 服务的作用
- 理解 DHCP 的工作过程
- 掌握 DHCP 服务器的配置和管理方法
- 掌握 DHCP 客户机的配置方法
- 掌握备份和还原 DHCP 数据库的方法

MEMO

7.1 知识介绍——DHCP 概述

动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）是用于为 TCP/IP 网络中的计算机自动分配 TCP/IP 参数的协议，有效地避免了因手动设置 IP 地址所产生的错误，同时也避免了把一个 IP 地址分配给多台计算机所造成的地址冲突，降低了配置 IP 地址的工作量。DHCP 的网络结构如图 7-1 所示。

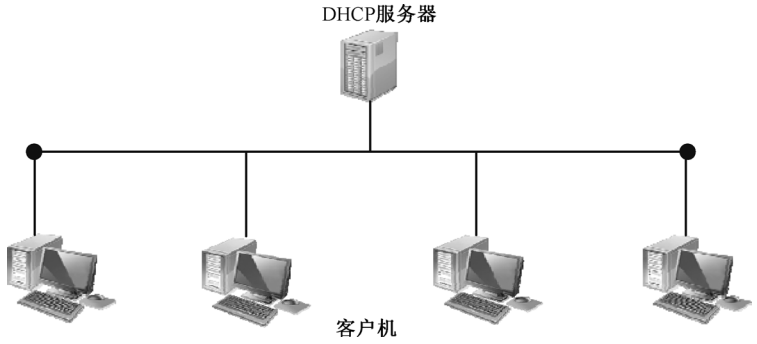


图 7-1 DHCP 网络的结构图

使用 DHCP 有以下优点：

- 减小管理员的工作量，提高了 IP 地址的利用率。
- 避免可能的输入错误，避免 IP 地址冲突。
- 当网络更改 IP 地址段时，不需要重新配置每台计算机的 IP 地址。
- 计算机移动时不用再重新配置 IP 地址。

7.1.1 DHCP 的租约过程

客户机从 DHCP 服务器获得 IP 地址的过程称为 DHCP 的租约过程。租约过程分为 4 个步骤，分别为：客户机请求 IP 地址、服务器响应请求、客户机选择 IP 地址和服务器确定租约，如图 7-2 所示。

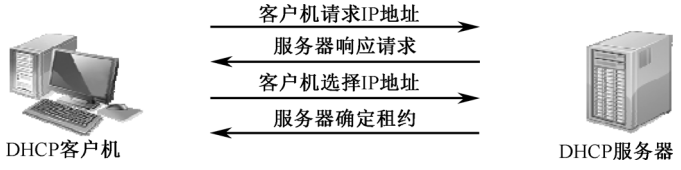


图 7-2 DHCP 的租约过程

1. 客户机请求 IP 地址

DHCP 客户机在网络中广播一个 DHCP Discover 包以请求 IP 地址，所以此过程也被称为 DHCP Discover。DHCP Discover 包的源 IP 地址为 0.0.0.0，目的 IP 地址为 255.255.255.255，该包还包含客户机的 MAC 地址（网卡地址）和计算机名，使 DHCP 服务器能够确定该请求

是哪个客户机发送的。客户机请求 IP 地址如图 7-3 所示。

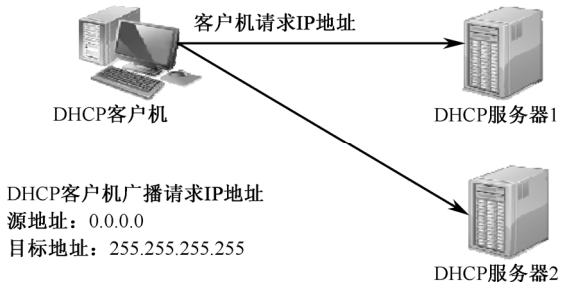


图 7-3　客户机请求 IP 地址

2．服务器响应请求

当 DHCP 服务器接收到客户机请求 IP 地址的信息时，就在自己的 IP 地址池中查找是否有合法的 IP 地址提供给客户机，如果有，DHCP 服务器就对此 IP 地址做标记，广播一个 DHCP Offer 包，此过程称为 DHCP Offer。DHCP Offer 包中包含以下信息。

- DHCP 客户机的 MAC 地址，用来正确标识客户机。
- DHCP 服务器提供的合法 IP 地址。
- 子网掩码。
- 租约期限。
- 服务器标识符（DHCP 服务器的 IP 地址）。
- 其他可选参数（如网关和 DNS 服务器地址）。

由于 DHCP 客户机还没有 IP 地址，所以由 DHCP 服务器发送广播消息。服务器响应请求如图 7-4 所示。如果网络中存在多台 DHCP 服务器，则这些服务器都会广播 DHCP Offer 包。

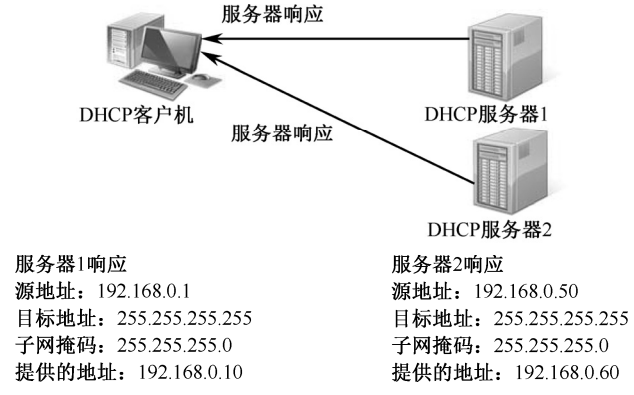


图 7-4　服务器响应请求

3．客户机选择 IP 地址

DHCP 客户机从接收到的第一个 DHCP Offer 包中选择 IP 地址，并将 DHCP Request 包广播到所有的 DHCP 服务器，表明它接受提供的内容，此过程称为 DHCP Request。DHCP Request 包的信息包含为该客户机提供 IP 配置的服务器的服务标识符（IP 地址）。DHCP 服务器查看服务器标识符字段，以确定自己提供的 IP 地址是否被客户机选中。如果客户机接收了 IP 地

址，则发出 IP 地址的 DHCP 服务器将该地址保留，该地址就不能再提供给另一个 DHCP 客户机；如果那些 DHCP Offer 包被拒绝，DHCP 服务器则取消提供并保留其 IP 地址，以用于下一个 IP 租约请求。客户机选择 IP 地址如图 7-5 所示。

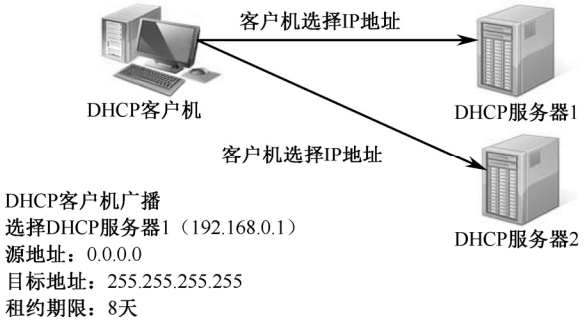


图 7-5　客户机选择 IP 地址

注意：

在客户机选择 IP 地址的过程中，虽然客户机选择了 IP 地址，但是还没有配置 IP 地址，所以源地址仍为 0.0.0.0，而在一个网络中可能有几个 DHCP 服务器，所以 DHCP 客户机仍然以广播方式发出 DHCP Request 包。

4．服务器确认 IP 租约

DHCP 租约过程中的最后一步是服务器确认 IP 租约，称为 DHCP ACK/DHCP Nack。DHCP 服务器接收到 DHCP Request 后，以 DHCP ACK（DHCP ACKnowledge）消息的形式向客户机广播成功信息，该消息包含 IP 地址的有效租约和其他可能配置的信息。当客户机收到 DHCP ACK 包时，它就配置 IP 地址，完成 TCP/IP 的初始化，从而可以在 TCP/IP 网络上通信。服务器确认 IP 租约如图 7-6 所示。如果服务器收到 DHCP Request 后，认为客户的请求是无效的，服务器会以 DHCP Nack 包响应。客户收到 DHCP Nack 包后会重新发送 DHCP Discover 包。

图 7-6　服务器确认 IP 租约

7.1.2　更新与释放租约

1．租约的更新

当客户机重新启动或者租期达到 50%时，就需要重新更新租约，客户机直接向提供租约的服务器发送 DHCP Request 包，要求更新现有的地址租约。如果 DHCP 服务器收到请求，

它将发送 DHCP 确认信息给客户机，更新客户机租约。如果客户机无法与提供租约的服务器取得联系，则客户机仍然可以继续使用原来的 IP 地址，一直等到租期到达 87.5%时，它将向网络上所有的 DHCP 服务器广播 DHCP Request 包，以更新现有的地址租约。如果有服务器响应客户机的请求，那么客户机将使用该服务器提供的地址信息更新现在的租约。如果仍然无法更新租约并且租约到期，客户机将放弃正在使用的 IP 地址，开始新的请求 IP 地址的租约过程。

在客户机上使用 ipconfig/renew 命令可以向 DHCP 服务器发送 DHCP Request 包，以接收更新选项和租约时间。

2. 租约的释放

在客户机上使用 ipconfig/release 命令，使 DHCP 客户机向 DHCP 服务器发送 DHCP Release 包并释放其租约。当移动客户机移动到不同的网络并且客户机不需要以前的租约时，这是很有用的。发布该命令后，客户机的 TCP/IP 通信联络将停止。

如果客户机在租约时间内保持关闭（并且不更新租约），那么在租约到期以后，DHCP 服务器可能将客户机的 IP 地址分配给其他的客户机。如果客户机不发送 DHCP Release 包，那么它在重新启动时，仍可尝试继续使用上一次使用过的 IP 地址。

7.2　任务 1：配置 DHCP 服务

ABC 公司网络内的计算机一直使用静态 IP 地址，均由管理员手动配置，所以经常出现 IP 地址冲突现象。为了改善这一状况，公司要配置一台 DHCP 服务器，用来为公司局域网内的计算机动态分配 IP 地址。

7.2.1　DHCP 安装要求

DHCP 服务可以安装在 Windows 操作系统的所有服务器版本上，本章在 Windows Server 2008 R2 操作系统上安装和配置 DHCP 服务。安装 DHCP 服务器需要满足如下要求。

- 服务器应具有静态 IP 地址。
- 在域环境下需要使用活动目录服务授权 DHCP 服务，以防止未经授权的 DHCP 服务器在网络中分配 IP 地址。
- 建立作用域（作用域是一段 IP 地址的范围）并激活。

在安装 DHCP 服务之前，需要规划以下信息。

- 确定 DHCP 服务器应分发给客户端的 IP 地址范围和子网掩码。
- 确定 DHCP 服务器不应向客户端分发的所有 IP 地址，应该保留一些固定 IP 地址给打印服务器、文件服务器等使用。
- 决定 IP 地址的租用期限，默认值为 8 天。

7.2.2　安装 DHCP 服务

使用 Windows Server 2008 R2 在工作组环境下搭建 DHCP 服务的步骤如下所述。

STEP1 打开“开始”→“管理工具”→“服务器管理器”窗口，选择“角色”，如图 7-7 所示，单击窗口右侧的“添加角色”。

图 7-7 添加角色

STEP2 出现“开始之前”页面，单击“下一步”按钮，在“选择服务器角色”页面中选择安装“DHCP 服务器”， 如图 7-8 所示，单击“下一步”按钮。

图 7-8 安装 DHCP 服务器

STEP3 在“DHCP 服务器简介”页面中直接单击“下一步”按钮，在如图 7-9 所示的“选择网络连接绑定”页面中，选择“请选择此 DHCP 服务器将用于向客户端提供服务的网络连接”，单击“下一步”按钮。

图 7-9 选择网络连接绑定

STEP4 在“指定 IPv4 DNS 服务器设置”页面，不添加父域名和 DNS 服务器地址，直接单击“下一步”按钮。在出现的“指定 IPv4 WINS 服务器设置”页面中，选择“此网络上的应用程序不需要 WINS”，单击“下一步”按钮。在出现的“添加或编辑 DHCP 作用域”页面中单击“添加”按钮，在“添加作用域”对话框中输入作用域的名称、起始地址、结束地址和子网掩码，并选择“激活此作用域”，如图 7-10 所示。添加或编辑作用域完成后，在“添加或编辑 DHCP 作用域”页面可以查看录入的作用域信息。

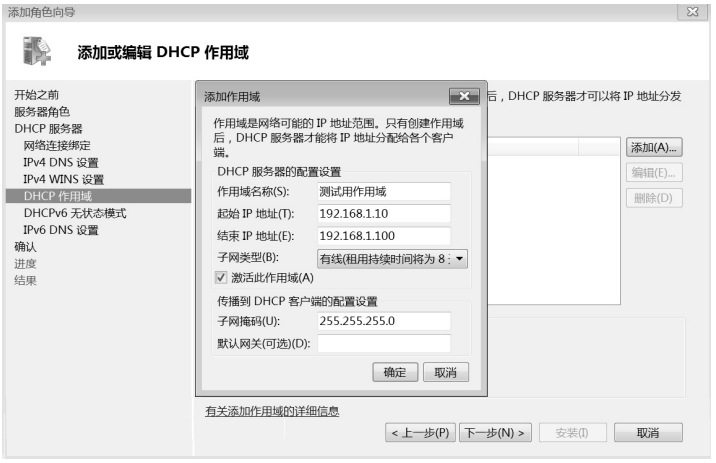


图 7-10　添加 DHCP 作用域

STEP5 在“配置 DHCPv6 状态模式”页面选择“对此服务器禁用 DHCPv6 无状态模式”，单击“下一步”按钮，如图 7-11 所示。

图 7-11　配置 DHCPv6 无状态模式

STEP6 在“确认安装选择”页面中会显示前面几步的配置信息，确认无误后单击“安装”按钮。安装完成后会在“安装结果”窗口显示安装是否成功及相关的提示信息，单击“关闭”按钮，完成整个安装配置过程。

7.2.3　授权 DHCP 服务器

授权是一种安全预防措施，它可以确保只有经过授权的 DHCP 服务器才能在网络中分配 IP 地址。

在域环境下搭建 DHCP 服务器时，可以直接在安装过程中为 DHCP 服务器授权，如图 7-12 所示，在“授权 DHCP 服务器”窗口，选择“使用当前凭据”或“使用备用凭据”，可以在安装时直接为 DHCP 服务器授权。

图 7-12　授权 DHCP 服务器

如果在“授权 DHCP 服务器”窗口中选择“跳过 AD DS 中此 DHCP 服务器的授权”，则可以在安装完成后使用 DHCP 控制台为该服务器授权。授权方法是打开 DHCP 控制台，右键单击服务器名称，选择“授权”，如图 7-13 所示。在域环境下，如果 DHCP 服务器没有授权，服务器下的 IPv4 和 IPv6 都会被标为红色下箭头，而且创建的作用域不能被激活。需要注意的是为 DHCP 服务器授权需要有企业管理员权限。

图 7-13　为 DHCP 服务器授权

7.2.4　配置作用域

作用域实际上就是一段 IP 地址范围，当 DHCP 客户机请求 IP 地址时，DHCP 服务器将从此段范围中选取一个尚未出租的 IP 地址，将其分配给 DHCP 客户机。每一个 DHCP 服务器中至少应有一个作用域，为一个网段分配 IP 地址。如果要为多个网段分配 IP 地址，就需要在 DHCP 服务器上创建多个作用域。

在 Windows Server 2008 R2 上安装 DHCP 服务时，默认情况下会创建一个作用域，安装完成后可以使用 DHCP 控制台创建多个作用域。

1. 新建作用域

STEP1 选择“开始”→“管理工具”→“DHCP”，打开 DHCP 管理控制台，展开左侧窗格的节点，右键单击“IPv4”，选择“新建作用域”，如图 7-14 所示。

图 7-14　新建作用域

STEP2 在向导页面单击“下一步”按钮，在“作用域名称”页面中输入作用域的名称，单击“下一步”按钮，如图 7-15 所示。

图 7-15　输入作用域的名称

STEP3 在“IP 地址范围”页面输入起始 IP 地址和结束 IP 地址以及子网掩码，单击“下一步”按钮，如图 7-16 所示。

图 7-16　输入 IP 地址范围

STEP4 在“添加排除和延迟”页面，输入需要排除的地址范围，然后单击“添加”按钮，单击“下一步”按钮，如图 7-17 所示。

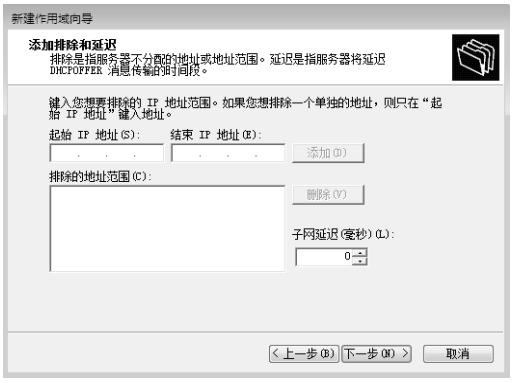


图 7-17　添加排除

STEP5 在“租用期限”页面指定 IP 地址的租期，这里采用默认的租用期限，单击“下一步”按钮，如图 7-18 所示。

图 7-18　指定地址的租期

STEP6 在“配置 DHCP 选项”页面选择“否，我想稍后配置这些选项”，单击“下一步”按钮，如图 7-19 所示。接下来在“完成新建作用域向导”窗口，单击“完成”按钮，完成新建作用域。

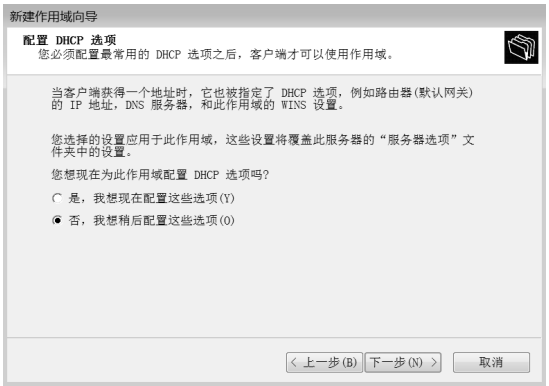


图 7-19　配置 DHCP 选项

2. 激活作用域

新建作用域之后，作用域前面有红色向下的箭头并且状态为不活动。此时客户端不能从该作用域获得 IP 地址（在作用域没有配置完整之前，防止客户机申请到不完整的 TCP/IP 信息）。配置完作用域的各项设置后，要使作用域生效，需要激活。激活的方法是右键单击作用域，选择“激活”，如图 7-20 所示。激活后作用域前面红色向下的箭头消失，如果需要停用该作用域，可以右键单击作用域，选择“停用”。

图 7-20　激活作用域

3. 配置作用域选项

创建 DHCP 作用域后，就可以为 DHCP 客户机配置选项（也可以在新建作用域过程中配置）。作用域选项可以给该作用域的客户机分配一些可选参数，如路由器（默认网关）的 IP 地址和 DNS 服务器的 IP 地址等。作用域选项只用于该作用域的客户机。配置作用域选项的步骤如下所述。

STEP1 在 DHCP 管理控制台窗口，展开要配置的作用域节点，右键单击目标作用域的“作用域选项”，选择“配置选项（C）…”，如图 7-21 所示。

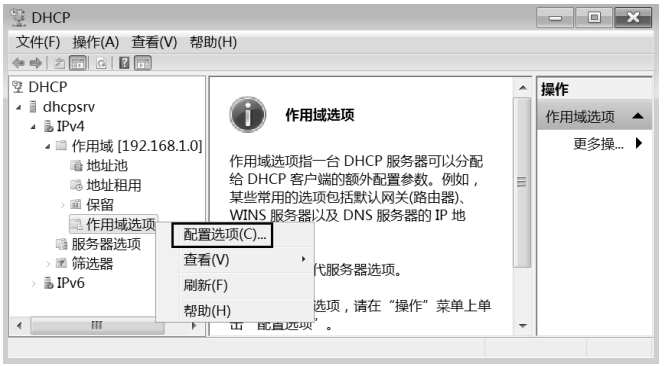


图 7-21　配置选项

STEP2 在打开的作用域选项对话框中选择“003 路由器”，输入路由器 IP 地址 192.168.1.5，选择“006 DNS 服务器”，输入 DNS 服务器的 IP 地址 202.97.224.68，依次单击“添加”和“确定”按钮，如图 7-22 所示。

图 7-22　输入路由器和 DNS 服务器地址

4. 配置客户端保留

客户端保留可以确保让某台 DHCP 客户机总是从 DHCP 服务器获得同一个 IP 地址，通常用于某些特殊的计算机（如文件服务器和打印服务器）。

STEP1 打开文件服务器（打印服务器）的“网络连接详细信息”，查看计算机网络适配器的 MAC 地址，如图 7-23 所示。

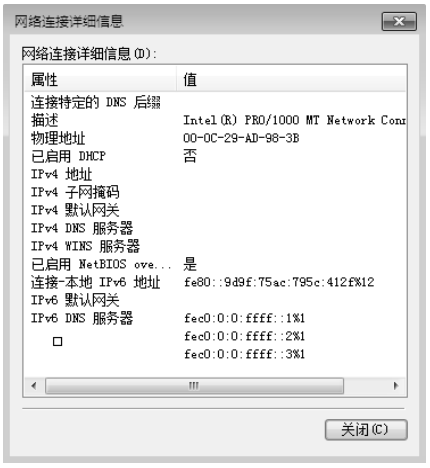


图 7-23　查看 MAC 地址

STEP2 在 DHCP 管理控制台中，右键单击作用域下的“保留”，选择“新建保留”，如图 7-24 所示。

STEP3 在“新建保留”对话框中输入为客户端保留的 IP 地址和客户端的 MAC 地址等保留信息，单击“添加”按钮，如图 7-25 所示。

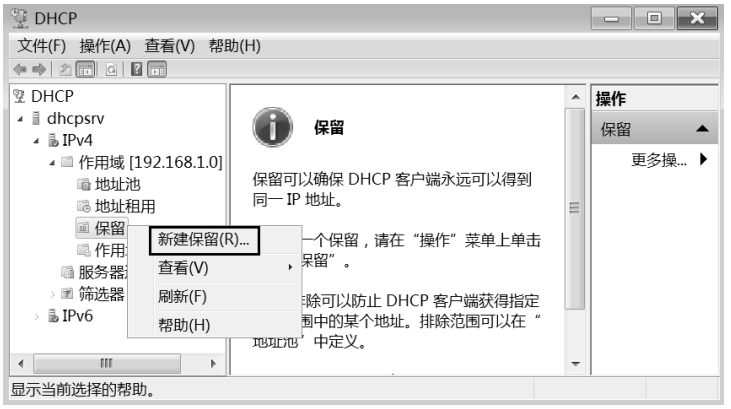


图 7-24　新建保留

图 7-25　输入保留信息

配置完客户端保留后，还可以为保留的地址配置选项，如 DNS 服务器地址和网关地址等。右键单击保留地址，选择“配置选项”，如图 7-26 所示，在“保留选项”对话框中配置所需的选项。

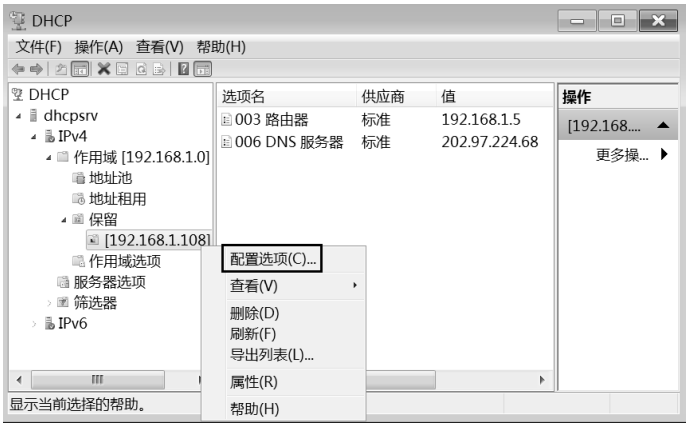


图 7-26　为保留地址配置选项

7.2.5 配置服务器选项

通过作用域选项的配置可知，当有多个作用域时，需要在各自的作用域下分别配置作用域选项。如果有些作用域选项是一样的，如公司网络中不同网段所配置的 DNS 服务器是相同的，那么就没有必要在各个作用域中配置，只需在服务器选项中配置。在 DHCP 控制台的左侧窗格展开节点树，右键单击 IPv4 下的“服务器选项”，选择“配置选项”，如图 7-27 所示，其他操作与配置作用域相同。

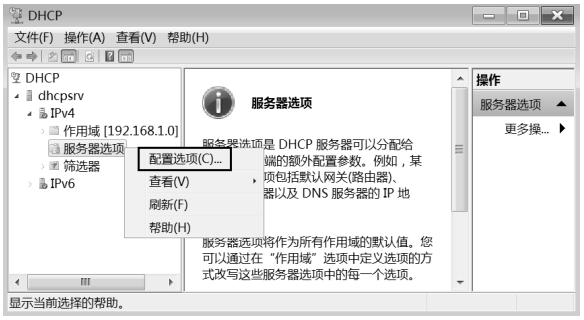


图 7-27 配置服务器选项

通过配置服务器选项、作用域选项和保留选项可知，各选项的功能都是配置客户机的 TCP/IP 参数的可选项，但各选项的应用范围和优先级不一样。服务器选项在本服务器上所有的作用域中生效，作用域选项在本作用域中生效，保留选项对保留的客户机生效。优先级别由高到低依次为：保留选项、作用域选项和服务器选项。

7.3 任务 2：配置 DHCP 客户机

以 Windows 7 客户机为例，具体步骤如下所述。

STEP1 将客户机的 IP 地址的获得方式和 DNS 服务器地址获得方式设置为自动获取，如图 7-28 所示。

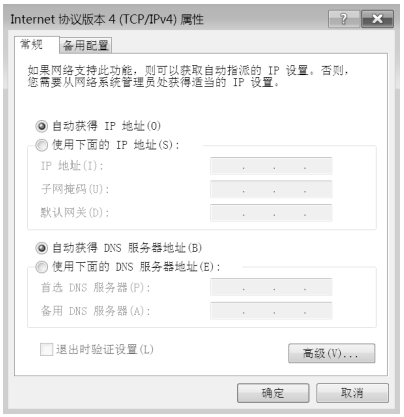


图 7-28 自动获得 IP 地址

STEP2 在客户端用 ipconfig/all 命令查看网络配置信息，检查是否获得 IP 地址以及相关选项设置，如图 7-29 所示，表示成功获得 IP 地址信息。其他 Windows 操作系统的客户端配置方法相同。

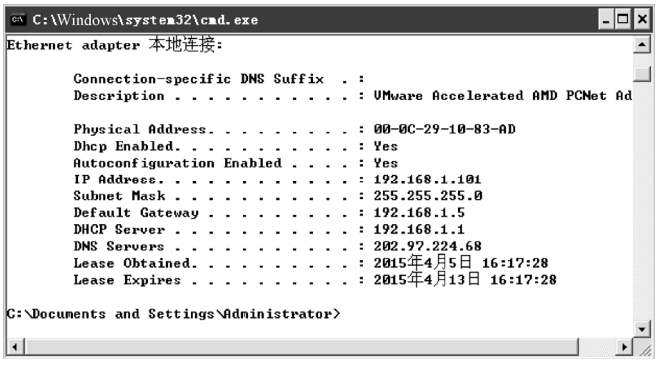


图 7-29　使用 ipconfig/all 查看网络配置信息

注意：

在客户机上可以运行“ipconfig/renew”命令来更新 IP 地址租约；如果不再使用获得的 IP 地址，可以运行“ipconfig/release”命令来释放 IP 地址。

如果客户端因故无法向 DHCP 服务器租到 IP 地址，客户端会每隔 5 min 自动搜索 DHCP 服务器，在未租到 IP 地址前，客户端默认为自己配置一个 169.254.0.0/16 格式的 IP 地址，此时可以在“备用配置”选项卡中为客户端设置另一个 IP 地址来替换 169.254.0.0/16 格式的 IP 地址，如图 7-30 所示。

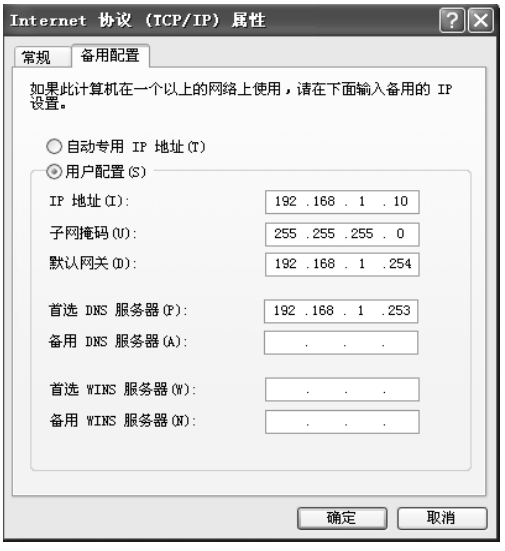


图 7-30　设置备用配置

- 自动专用 IP 地址：这是默认值，当计算机无法从网络上的 DHCP 服务器租到 IP 地址时，计算机会自动使用 169.254.0.0/16 格式的专用 IP 地址。
- 用户配置：当客户端无法从网络上的 DHCP 服务器租到 IP 地址时，计算机会自动使

用此处所指定的 IP 地址，此功能适合于客户端需要在不同网络中使用的情况。

当客户端从 DHCP 服务器获得 IP 地址后，可以在 DHCP 服务器上查看地址租用信息。打开 DHCP 管理控制台，选择作用域下的“地址租用”，可以查看到有多少个客户端从该服务器获得 IP 地址，以及客户端获得的 IP 地址和租用截至日期等信息，如图 7-31 所示。

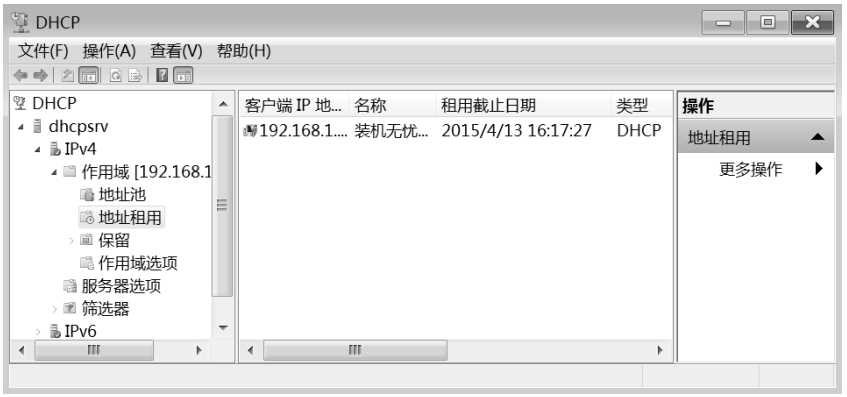


图 7-31　地址租用信息

7.4　任务 3：维护 DHCP 服务器

在工作环境中，DHCP 服务器会因为各种软、硬件故障造成服务停止或服务器宕机。为了能在发生故障时快速恢复 DHCP 服务并且使用原有配置，需要定期备份 DHCP 数据库，以便使用备份恢复原有配置。

1. 备份 DHCP 数据库

备份 DHCP 数据库的步骤如下所述。

STEP1 打开 DHCP 管理控制台，在左侧窗格中右键单击服务器名称，选择“备份”，如图 7-32 所示。

图 7-32　选择备份

STEP2 在“浏览文件夹”对话框中，选择备份文件的路径，单击“确定”按钮，完成备份，如图 7-33 所示。

图 7-33　选择备份文件的路径

2. 使用备份还原 DHCP

使用备份还原 DHCP 的步骤如下所述。

STEP1 在目标服务器上添加DHCP服务器角色，不做任何配置（如果是域环境则需要授权），复制备份文件至目标服务器。

STEP2 在目标服务器上打开 DHCP 控制台，右键单击服务器名称，选择“还原”，如图 7-34 所示。

图 7-34　选择还原

STEP3 在“浏览文件夹”窗口中，选择备份所在的文件夹，单击“确定”按钮。系统提示必须停止和重新启动服务，单击“是”按钮，如图 7-35 所示。

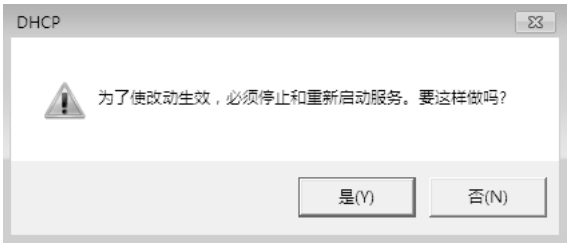


图 7-35　重启服务

STEP4 还原成功后，新建的 DHCP 将直接使用原有的配置信息，减少了配置工作，加快了恢复速度，并且避免了因配置错误导致的 IP 地址冲突，如图 7-36 所示。

图 7-36 还原成功

7.5 实训

实训环境一

HT 公司在局域网内使用 DHCP 服务器为计算机提供 IP 地址，局域网使用 192.168.1.0/24 网段，其中 192.168.1.1～192.168.1.10 保留给服务器使用，192.168.1.11～192.168.1.200 分配给 190 台客户机使用，剩下的 54 个 IP 地址保留。默认网关为 192.168.1.1，DNS 服务器为 192.168.1.2，规划 DHCP 服务器的地址为 192.168.1.3。

需求描述

- 添加 DHCP 服务器角色。
- 配置 DHCP 服务器授权，以确保只有经过授权的 DHCP 服务器才能在网络中运行。
- 创建和配置 DHCP 作用域，使客户机可以向服务器请求 IP 地址。

实训环境二

HT 公司的 DHCP 服务器因为硬件故障突然宕机了，并且需要长时间停机维护。为了保证公司内部网络的正常运行，需要快速恢复 DHCP 服务应该如何实现？

需求描述

- 平时定期备份 DHCP 数据库。
- 当 DHCP 服务器宕机时，在另一台服务器上安装 DHCP 服务角色。
- 在替代计算机上使用备份恢复 DHCP 服务。

7.6　习题

- DHCP 租约要经过哪些过程？
- DHCP 服务器要具备哪些条件？
- 在什么情况下，需要进行 DHCP 服务器的授权？
- 如何设置 DHCP 客户机？如何检测 DHCP 客户机获得的动态 IP 地址及其他信息？
- DHCP 作用域的“保留”选项具有什么功能？它与作用域的排除地址有何不同？

第 8 章

配置 DNS 服务

项目需求：

ABC 公司需要一台 DNS 服务器为内部用户提供域名解析，用户可以使用域名访问公司的网站。为了提高冗余性，公司还需要搭建第二台 DNS 服务器，将第一台 DNS 服务器上的记录传输到第二台 DNS 上。内部的局域网使用 abc.com 作为域名后缀，现在该公司在上海成立分公司，上海分公司使用专线和总公司连接。上海分公司需要使用 sh.abc.com 作为域名后缀。

技能目标：

- 了解域名空间结构
- 理解 DNS 查询过程
- 掌握 DNS 区域管理方法
- 掌握转发器的配置方法
- 理解子域和委派

MEMO

8.1 知识介绍——DNS 概述

在网络通信中，由于 IP 地址信息不容易记忆，所以网络中出现了域名这个概念，在访问时我们只需要输入好记忆的域名即可。DNS 是域名系统（Domain Name System）的缩写，通过为每台主机建立 IP 地址与域名之间的映射关系，避开难记的 IP 地址，使用域名来唯一标识网络中的计算机。

8.1.1 域名空间

在 DNS 中，域名空间采用分层结构，包括根域、顶级域、二级域和主机名。域名空间的层次结构类似一棵倒置的树，其中根作为最高级别，树枝处于下一级级别，树叶则处于最低级别。一个区域就是 DNS 域名空间中的一部分，维护着该区域的数据库记录。在域名层次结构中，每一层称作一个域，每个域用一个点号“.”分开。域又可以进一步分成子域，每个域都有一个域名，最底层是主机，DNS 网络结构图如图 8-1 所示。

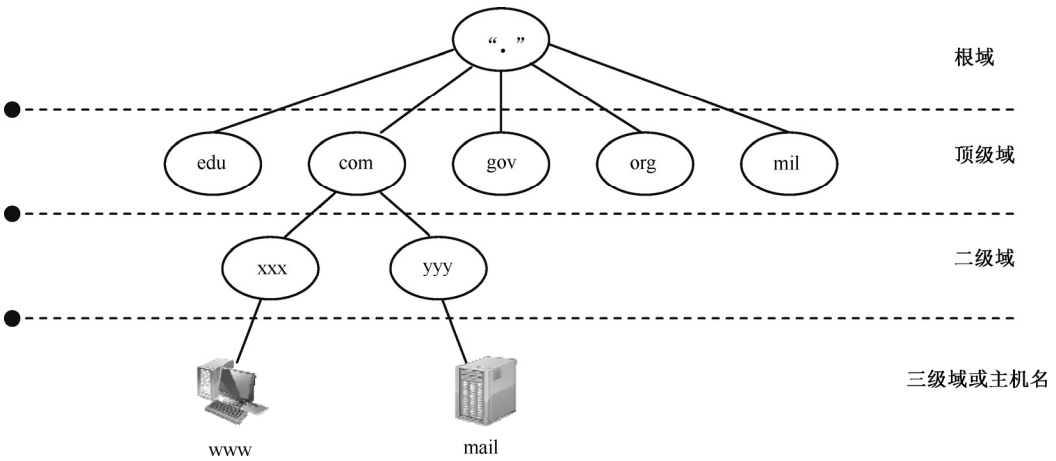


图 8-1 DNS 网络结构图

注意：

三级域名下面还可以有四级域名和五级域名等，但是域名层级越多，域名就越复杂，越不易使用，所以在实际使用中，一般不会超过五级。

1. 根域

参照图 8-1，根（Root）域就是“.”点号，它由 Internet 名字注册授权机构管理，该机构把域名空间各部分的管理责任分配给连接到 Internet 的各个组织。

2. 顶级域

DNS 根域的下一级是顶级域，由 Internet 名字授权机构管理，共有 3 种类型的顶级域。

- 组织域：采用 3 个字符的代号，表示 DNS 域中所包含的组织的主要功能或活动，如表 8-1 所示。

表 8-1　组织域

顶 级 域 名	说　　明
gov	政府部门
com	商业部门
edu	教育部门
org	民间团体组织
net	网络服务机构
mil	军事部门

- 国家或地区域：采用两个字符的国家或地区代号，如表 8-2 所示。
- 反向域：反向域是一个特殊域，名称为 in-addr.arpa，用于将 IP 地址映射到域名。

表 8-2　国家或地区域

顶 级 域 名	国别 / 地区
cn	中国
jp	日本
uk	英国
au	澳大利亚
hk	中国香港
…	…

3. 二级域

二级域是注册到个人、组织或公司的名称。这些名称基于相应的顶级域，如“Microsoft.com”，就是基于顶级域“.com”。二级域下可以包括主机和子域，如“Microsoft.com”可包含如“ftp.microsoft.com”这样的主机，也可以包含如“www.microsoft.com”这样的子域，而该子域还可以包含如“printer1.www.microsoft.com”这样的主机。

4. 主机名

主机名处于域名空间结构中的最底层，主机名和前面讲的域名（DNS 后缀）结合构成 FQDN（Full Qualified Domain Name，完全合格的域名），主机名是 FQDN 最左端的部分。例如，“xxx.yyy.com.”中的“xxx”是主机名，“yyy.com.”被称为 DNS 后缀。DNS 后缀最右边的“.”代表根域，因为根域是域名结构的最顶层，所以，在实际应用中，可以将最右边的“.”省略，简写成“xxx.yyy.com”。

用户在互联网上访问 Web、FTP 和 Mail 等服务时，通常使用 FQDN 进行访问，例如，www.abc.com，但是 FQDN 并不能真正地定位目标服务器的位置，而是需要 DNS 服务器将 FQDN 解析成 IP 地址。

8.1.2 DNS 查询模式

DNS 服务的主要作用就是将域名解析为 IP 地址。例如，客户机使用 FQDN 访问 Web 服务器，需要解析出 Web 服务器的 IP 地址。首先客户机向 DNS 服务器发送域名查询请求，然后 DNS 服务器告知客户机 Web 服务器的 IP 地址，最后客户机与 Web 服务器通信。DNS 查询如图 8-2 所示。

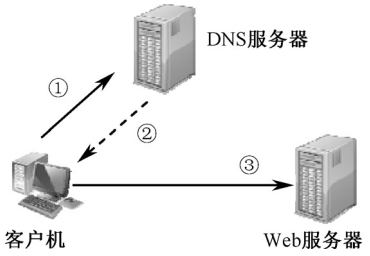


图 8-2 DNS 查询

在互联网上，有许多 DNS 服务器负责域名到 IP 地址的解析。域名系统是一个遍布在互联网上的分布式主机信息数据库系统，采用客户机 / 服务器的工作模式。

1. DNS 查询过程

下面通过查询域名 www.abc.com 的例子来说明 DNS 查询的基本工作原理，具体步骤如图 8-3 DNS 查询过程所示。

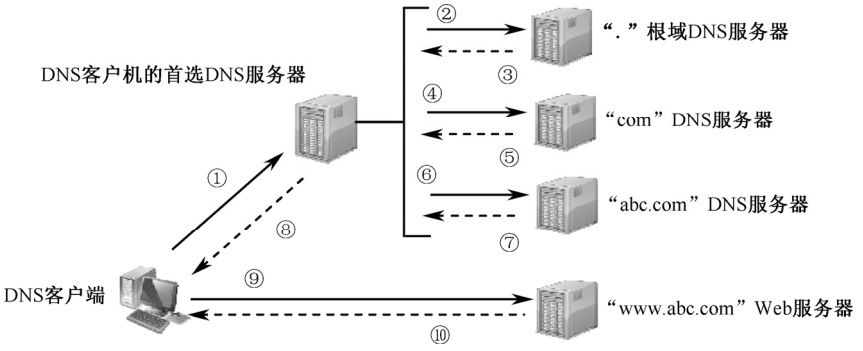


图 8-3 DNS 查询过程

① 客户机将查询 www.abc.com 的信息传递到自己的首选 DNS 服务器。

② DNS 客户机的首选 DNS 服务器检查区域数据库，由于此服务器没有 abc.com 域的授权记录，因此，它将查询信息传递到根域 DNS 服务器，请求解析主机名称。

③ 根域 DNS 服务器把负责解析“com”顶级域的 DNS 服务器的 IP 地址返回给 DNS 客户机的首选 DNS 服务器。

④ 首选 DNS 服务器将请求发送给负责“com”域的 DNS 服务器。

⑤ 负责“com”域的服务器根据请求将负责“abc.com”域的 DNS 服务器的 IP 地址返回给首选 DNS 服务器。

⑥ 首选 DNS 服务器向负责“abc.com”区域的 DNS 服务器发送请求。

⑦ 由于此服务器具有 www.abc.com 的记录，因此它将 www.abc.com 的 IP 地址返回给首选 DNS 服务器。

⑧ 客户机的首选 DNS 服务器将 www.abc.com 的 IP 地址发送给客户机。

⑨ 域名解析成功后，客户机将 HTTP 请求发送给 Web 服务器。

⑩ Web 服务器响应客户机的访问请求，客户机便可以访问目标主机。

如果 DNS 客户机的首选 DNS 服务器没有返回给客户机 www.abc.com 的 IP 地址，那么客户机将尝试访问自己的备用 DNS 服务器。

为了提高解析效率，减少查询开销，每个 DNS 服务器都有一个高速缓存，存放最近解析过的域名和对应的 IP 地址。这样，当有用户查找相同的域名记录时，便可以跳过某些查找过程，DNS 服务器直接从缓存中查找到该记录的地址，大大缩短了查找时间，加快了查询速度。

2. DNS 区域

除了将域名系统（DNS）的命名空间划分为域，还可以将 DNS 的命名空间划分为区域，其中存储有关一个或多个 DNS 域的名称信息。例如，在一个区域中包含的每个 DNS 域名的信息，该区域是否为权威来源等。

开始时，区域为单个 DNS 域名。如果在初始域下面添加了其他域，则这些域可以作为相同区域的部分或属于其他区域。即当添加子域时，可以将其作为一部分包含在原始区域中，也可以将其委派到为支持该子域而创建的其他区域。

DNS 区域示意图如图 8-4 所示，该图显示了“abc.com”区域，该区域可以包括“abc.com”所有的 DNS 名称空间。然而，如果这个“abc.com”区域需要使用子域，则这些子域必须包含在该区域中或委派到另一个区域。

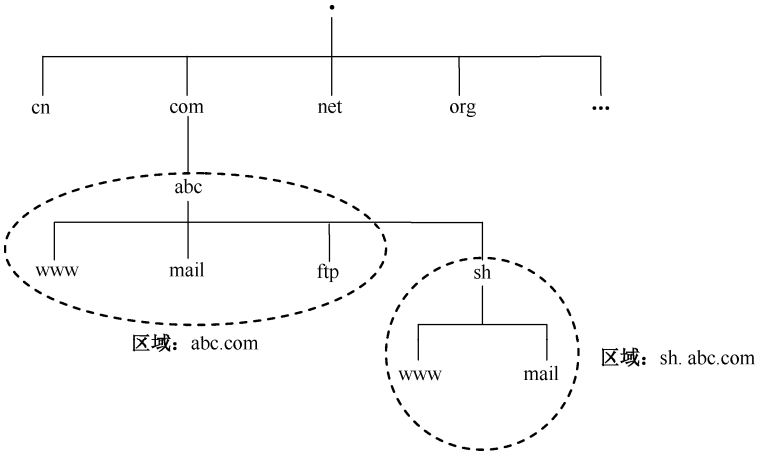


图 8-4　DNS 区域示意图

3. 递归查询和迭代查询

在 DNS 查询过程中有两种查询类型：递归查询和迭代查询。

（1）递归查询

递归查询是最常见的查询方式， 当 DNS 客户端按照它的 DNS 服务器列表向 DNS 服务器发出查询请求时，接受查询请求的 DNS 服务器和客户端之间的查询关系一般都是递归查询。该 DNS 服务器会查询自己的区域文件和缓存，如果没有找到结果，就向别的 DNS 服务器查询。当采用递归查询时，客户端得到的结果只能是成功或失败，接受查询请求的 DNS 服务器必须告诉客户端请求查询的 IP 地址或者告诉客户端找不到请求的地址及找不到的原因（查询超时或遇到错误）。图 8-3 中 DNS 客户端提出的查询请求属于递归查询。

（2）迭代查询

迭代查询又称为简单查询，是指 DNS 服务器根据自己的高速缓存或区域的数据，以最佳结果回答。如果 DNS 服务器无法解析，它可能返回一个指针，该指针指向可能有目标域名记录的 DNS 服务器，继续该过程，直到找到拥有目标记录的 DNS 服务器，或者直到查询出错或超时为止。DNS 服务器与 DNS 服务器之间的查询大部分属于迭代查询。在图 8-3 中，步骤②～⑤就属于迭代查询。

注意：

DNS 服务器之间一般都是发送迭代查询请求，除非 DNS 服务器接受了一个递归查询请求，并且无法解析该查询，这时该服务器将向转发器中的 DNS 服务器发送递归查询请求。如果没有设置转发器，该服务器将向根提示中的根服务器发送迭代查询的请求。

4．正向查询和反向查询

DNS 服务器的域名查询从查询内容上分，可以分为两种形式：正向查询和反向查询。

- 正向查询是由域名查找 IP 地址。
- 反向查询是由 IP 地址查找域名。

反向搜索查询要求对每个域名进行详细搜索，这需要花费很长时间。为解决该问题，DNS 标准定义了一个名为 in-addr.arpa 的特殊域（反向域）。in-addr.arpa 域遵循域名空间的层次命名方案，它基于 IP 地址，而不是基于域名，其中，IP 地址 8 位组的顺序是反向的，例如，如果客户机要查找 172.16.44.1 的 FQDN，就查询反向域 44.16.172. in-addr.arpa 中的 PTR 指针记录。

8.2 任务 1：配置 DNS 服务器

在配置 DNS 服务器之前，首先要添加 DNS 服务器角色。配置 DNS 服务器包括创建正向和反向查找区域，以及配置 DNS 服务属性，如转发器等。

8.2.1 必要条件

DNS 服务器要为客户机提供域名解析服务，必须具备以下条件。

- 有固定的 IP 地址。
- 安装并启动 DNS 服务。
- 有区域文件，或者配置转发器，或者配置根提示。

8.2.2　安装 DNS 服务器角色

ABC 公司的内部局域网需要一台 DNS 服务器为内部用户提供域名解析，IP 地址为 192.168.1.1。在 Windows Server 2008 R2 系统搭建 DNS 服务的步骤如下所述。

STEP1 打开“开始”→“管理工具”→“服务器管理器”窗口，选择“角色”，单击右侧的“添加角色”。在“添加角色向导”中的“开始之前”页面单击“下一步”按钮，在选择“服务器角色”页面选择“DNS 服务器”，单击“下一步”按钮，如图 8-5 所示。

图 8-5　添加角色

STEP2 在“DNS 服务器简介”页面中直接单击“下一步”按钮，在“确认安装选择”页面单击“安装”按钮，开始安装 DNS 服务器。

STEP3 安装完成后显示安装成功，单击“关闭”按钮，完成安装过程。安装结果如图 8-6 所示。

图 8-6　安装结果

8.2.3　新建区域

安装好 DNS 服务器角色后，接下来需要新建区域。区域包括两种类型：正向查找区域和反向查找区域。正向查找区域就是通过 FQDN 查找 IP 地址，而反向查找区域就是通过 IP 地址查找 FQDN。本书将主要介绍正向查找区域的创建，创建反向查找区域与创建正向区域的方法相似，本书只进行简单介绍。

在创建区域时，有 3 种类型可供选择（正向查找区域和反向查找区域都有这 3 种类型）。

- “主要区域”：是新区域的正本，负责在新区域的计算机上管理和维护本区域的资源记录。如果这是一个新区域，则选择“主要区域”单选按钮。
- “辅助区域”：是现有区域的副本，主要区域中的 DNS 服务器将把区域信息传递给辅助区域中的 DNS 服务器。使用辅助区域的目的是提供冗余，减少包含主要区域数据库文件的 DNS 服务器的负载。辅助 DNS 服务器上的区域数据无法修改，所有数据都是从主 DNS 服务器复制而来的。
- “存根区域”：只包含少数记录，如 SOA、NS 与 A 记录，用于标识该区域的权威 DNS 服务器所需的资源记录。含有存根区域的 DNS 服务器对该区域没有管理权，它维护着该区域的权威 DNS 服务器列表，列表存在 DNS 资源记录中。

除了上面这 3 种类型可选，还有一个复选项“在 Active Directory 中存储区域（DNS 服务器是可写域控制器时才可用）”，此选项仅在 DNS 服务器是可写域控制器时才可能用，区域的数据存放在 Active Directory 中，可提高区域数据的安全性。

当创建的区域只用于局域网内而不用于 Internet 时，可以不用遵守域名空间的命名规则。例如，可以在局域网内创建一个名为 it. abc 的区域。但是当域名用于 Internet 时，必须遵守域名空间结构，而且使用的域名必须是经域名注册机构（例如，CNNIC，中国互联网信息服务中心）注册过的。

1．创建正向查找区域

STEP1 选择“开始”→“管理工具”→“DNS”，打开“DNS 管理器”窗口，如图 8-7 所示。

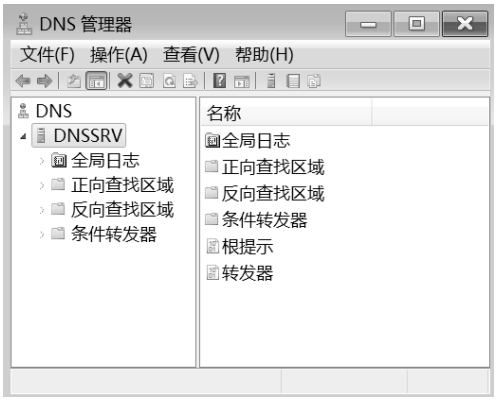


图 8-7 DNS 管理器

STEP2 在“DNS 管理器”窗口展开服务器名称节点，右键单击“正向查找区域”，选择“新建区域”，如图 8-8 所示。

STEP3 在“新建区域向导”页面单击“下一步”按钮，出现“区域类型”页面，选择“主要区域”，单击“下一步”按钮，如图 8-9 所示。

STEP4 在“区域名称”页面输入“abc.com”，单击“下一步”按钮，如图 8-10 所示。

STEP5 在“区域文件”页面使用默认设置，不修改文件名，单击“下一步”按钮，如图 8-11 所示。

STEP6 在“动态更新”页面选择“不允许动态更新”，单击“下一步”按钮，如图 8-12 所示。

图 8-8　新建区域

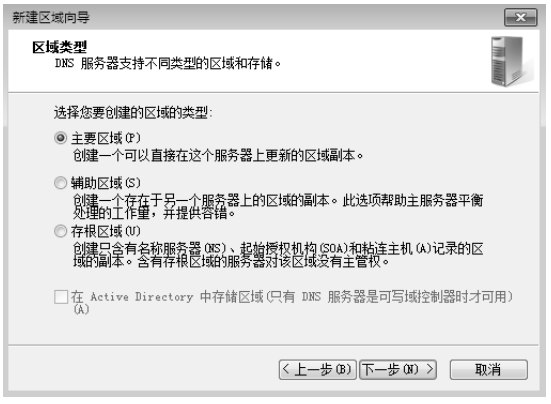


图 8-9　区域类型

图 8-10　区域名称

图 8-11　区域文件

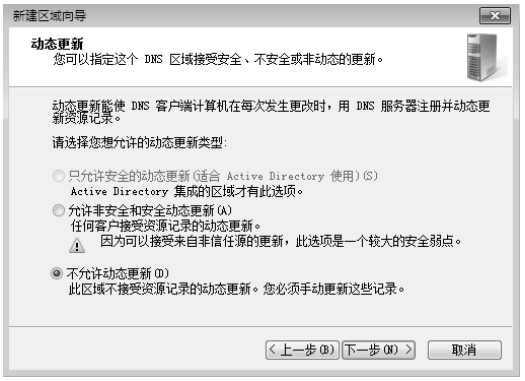


图 8-12　不允许动态更新

STEP7 在“正在完成新建区域向导”页面单击“完成”按钮，完成新建区域，如图 8-13 所示。

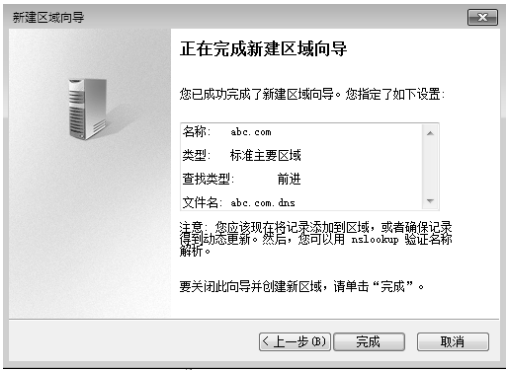


图 8-13　完成新建区域

2．创建反向查找区域

创建反向查找区域的步骤与正向查找区域类似，具体步骤如下所述。

STEP1 在“DNS 管理器”窗口右键单击“反向区域”，选择“新建区域”，在“区域类型”页面选择“主要区域”，在“反向查找区域名称”页面选择“IPv4 反向查找区域”，单击“下一步”按钮，如图 8-14 所示。

图 8-14　选择“IPv4 反向查找区域”

STEP2 在“反向查找区域名称”页面，输入网络 ID，即要查找的网段地址，单击“下一步”按钮，如图 8-15 所示。

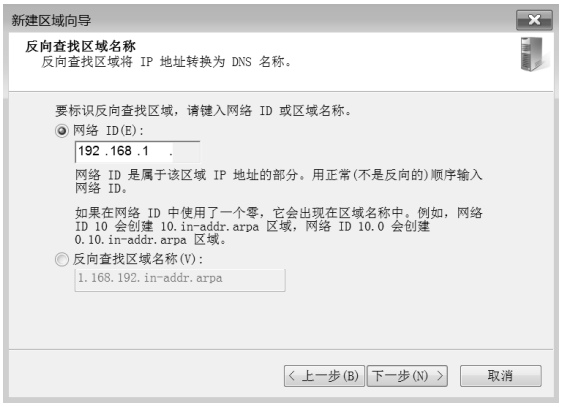


图 8-15　输入网络 ID

STEP3 在“区域文件”页面选择“新建区域文件”并使用默认文件名，单击“下一步”按钮。在“动态更新”页面选择“不允许动态更新”，单击“下一步”按钮。按照提示完成反向查找区域的创建。创建完反向查找区域后，就可以添加 PTR 指针记录，将 IP 地址解析成 FQDN。

8.2.4　创建资源记录

1. 资源记录类型

在完成 DNS 服务器查找区域的创建后，可以新建资源记录。在区域文件中包含许多种资源记录（Resource Record）。例如，将 FQDN 映射成 IP 地址的资源记录为 A 记录，将 IP 地址映射到域名的资源记录为 PTR 记录。DNS 上常用的资源记录如表 8-3 所示。

表 8-3　资源记录

资 源 记 录	说　　明
SOA（起始授权机构）	定义了该域中的权威名称服务器
NS（名称服务器）	表示某区域的权威服务器和 SOA 中指定的该区域的主服务器和辅助服务器
A（主机）	列出了区域中 FQDN（完全合格的域名）到 IP 地址的映射
PTR（指针）	相对于 A 资源记录，PTR 记录是把 IP 地址映射到 FQDN
MX	邮件交换器记录，向指定的邮件交换主机提供消息路由
SRV（服务）	列出了正在提供特定服务的服务器
CNAME（别名）	将多个名字映射到同一台计算机上，便于用户访问

2. 新建主机记录

ABC 公司的网站域名为 www.abc.com，IP 地址为 192.168.1.2，在区域 adb.com 下创建该主机记录的步骤如下。

在“DNS 管理器”窗口右键单击正向查找区域“abc.com”，选择“新建主机（A 或 AAAA）”，如图 8-16 所示。

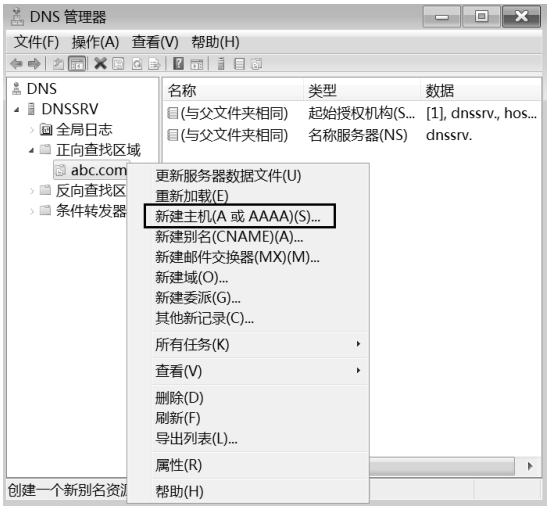


图 8-16　新建主机记录

在“新建主机”页面中输入主机的名称“WWW”和 IP 地址 192.168.1.2，单击“添加主机”，完成新建主机记录，如图 8-17 所示。

3．新建主机的别名记录

有时需要为一台主机创建多个主机名，可以利用添加别名资源记录来达到这个目的。在图 8-16 所示的快捷菜单中选择“新建别名（CNAME）”，在“新建资源记录”页面输入别名和目标主机的 FQDN，单击“确定”按钮，完成新建别名记录，如图 8-18 所示。

别名记录不仅可以和源主机记录在同一区域内，而且还可以将别名记录建立在不同的区域上，但是需要确保 DNS 服务器能正确解析源主机记录。

图 8-17　输入主机的名称和地址

图 8-18　新建别名

8.3　任务 2：配置 DNS 客户机

配置 DNS 客户机是为客户机指定 DNS 服务器的 IP 地址，从而使用它们可以请求 DNS 服务。客户机可以配置静态 DNS 服务器地址或者是动态获得 DNS 服务器地址。

打开“本地连接属性”对话框，选择“Internet 协议版本 4”，单击“属性”。在打开的“Internet 协议版本 4 属性”对话框中，选择“使用下面的 DNS 服务器地址”，输入 DNS 服务器的 IP 地址，单击“确定”按钮，如图 8-19 所示。

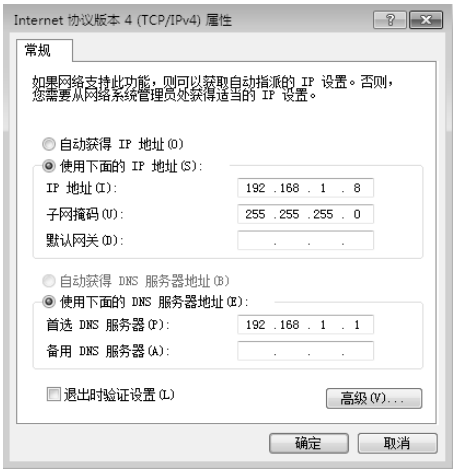


图 8-19　输入 DNS 服务器地址

动态获得 DNS 服务器地址，需要与 DHCP 服务结合起来，在 DHCP 服务器上为 DHCP 客户机配置 DNS 信息。

在 DNS 客户机上，可以使用“ping 域名”的方法查看域名解析是否正确。检查域名解析如图 8-20 所示，由图中可以看出，已经得知 www.abc.com 的 IP 地址为 192.168.1.2。

图 8-20　检查域名解析

注意：

Windows 操作系统中在“%systemroot%\system32\drivers\etc”文件夹中有一个 hosts 文件，提供了一个简单的 IP 地址和域名的映射，一般用于实验测试，免去构建 DNS 服务器的烦琐工作。

8.4 任务 3：高级设置

8.4.1 转发器

1. 转发器简介

DNS 服务器可以解析自己区域文件中的域名，对于本服务器查询不了的域名，默认情况下将直接转发查询请求到根域 DNS 服务器。除此之外，还可以在 DNS 服务器上设置转发器，将请求转发给其他 DNS 服务器。

对于本地 DNS 服务器（在局域网中）无法解析的域名查询，可以通过配置转发器的方法来实现域名解析，DNS 转发示意图如图 8-21 所示，在本地 DNS 服务器上设置转发器，指向互联网上的 DNS 服务器。

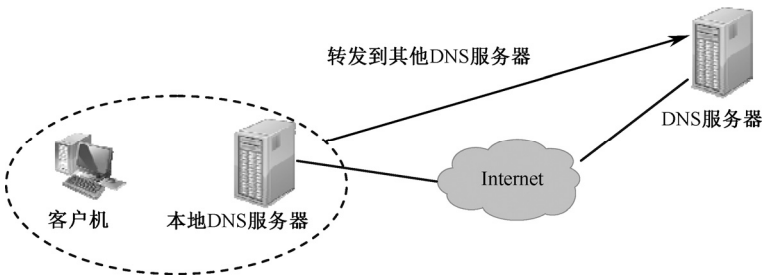


图 8-21 DNS 转发示意图

2. 配置 DNS 转发器

转发器是网络上的一个域名系统（DNS）服务器，它将把对外部 FQDN 的查询请求转发给网络外部的 DNS 服务器，还可以使用条件转发器按照特定域名转发查询请求。

在 Windows Server 2008 R2 系统配置 DNS 服务转发器的步骤如下所述。

STEP1 使用管理员账户登录 DNS 服务器，在“DNS 管理器”窗口右键单击服务器名称，选择“属性”，如图 8-22 所示。

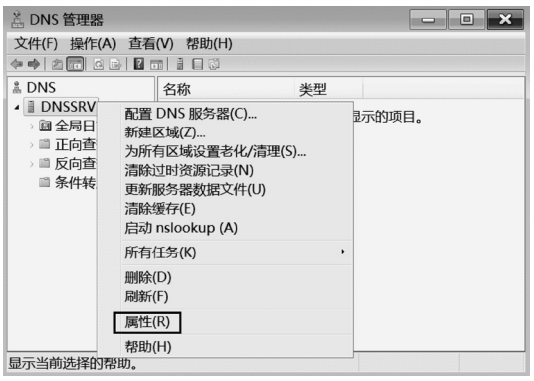


图 8-22 DNS 服务器“属性”

STEP2 在“DNS SVR 属性”页面中选择“转发器”选项卡，如图 8-23 所示，单击“编辑”按钮。

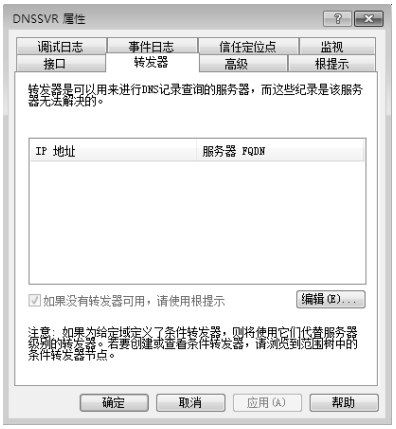


图 8-23　“转发器”选项卡

STEP3 在“编辑转发器”页面中输入远端 DNS 服务器地址，单击“确定”按钮，如图 8-24 所示。

图 8-24　输入远端 DNS 服务器地址

STEP4 如果设置正确，系统会自动解析出远端 DNS 服务器的 FQDN，如图 8-25 所示。

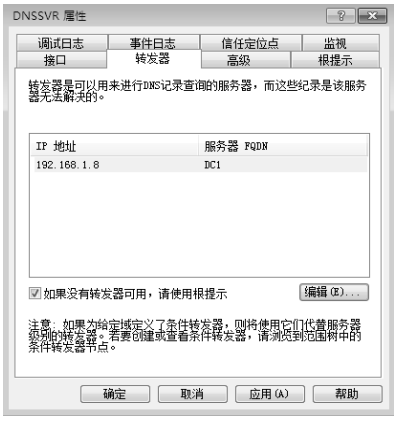


图 8-25　自动解析远端 DNS 服务器的 FQDN

8.4.2 DNS 区域传输

为了减轻单台 DNS 服务器的负载，有时要将一台 DNS 服务器的内容保存在多台 DNS 服务器中。这时，就要用到 DNS 的“区域传输”功能。“区域传输”就是从主服务器上将区域文件的信息复制到辅助服务器上。

主服务器是区域传输的来源服务器，它既可以是主要区域，又可以是辅助区域。如果主服务器是主要区域，区域传输则直接从主要区域取得区域文件；如果主服务器是辅助区域，区域传输则仅传输区域文件的一个只读副本。

在 Windows Server 2008 R2 系统配置 DNS 区域传输的步骤如下所述。

STEP1 在第一台 DNS 服务器上的“DNS 管理器”窗口中，右键单击需要复制的区域，选择“属性”命令，打开区域属性页面，打开“区域传送”选项卡，选择“允许区域传送”下的“只允许到下列服务器”，如图 8-26 所示，单击“编辑”按钮。

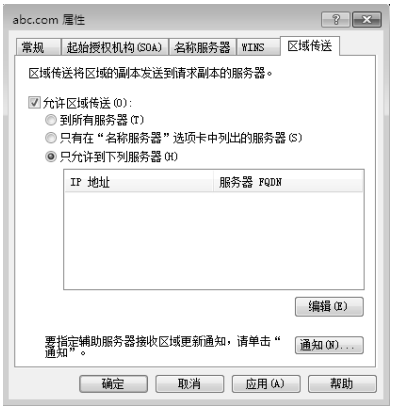


图 8-26 区域属性

STEP2 在“允许区域传送”页面输入辅助服务器的 IP 地址，验证成功后单击“确定”按钮，如图 8-27 所示。

图 8-27 输入辅助服务器的地址

STEP3 在辅助服务器（第二台 DNS）上建立正向查找区域，在“区域类型”窗口选择“辅助区域”，单击“下一步”按钮，如图 8-28 所示。

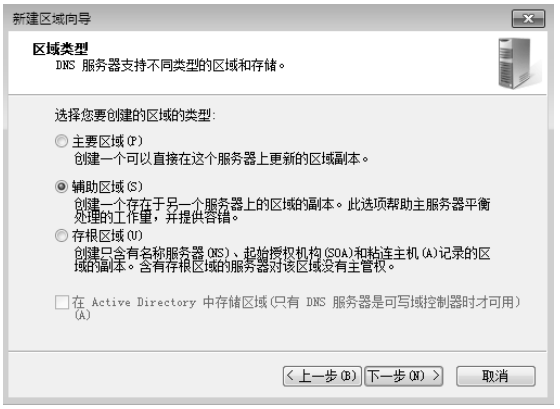


图 8-28　建立辅助区域

STEP4 在“区域名称”窗口输入辅助区域的名称，需要和源区域完全相同，单击“下一步”按钮，如图 8-29 所示。

图 8-29　输入辅助区域的名称

STEP5 输入主服务器的 IP 地址，验证后单击“下一步”按钮，如图 8-30 所示。

图 8-30　输入主服务器的 IP 地址

STEP6 在“正在完成新建区域向导”窗口单击“完成”按钮，完成辅助区域创建，如图 8-31 所示。展开辅助服务器的“DNS 管理器”节点树，查看 abc.com 区域，数据已经复制完成。

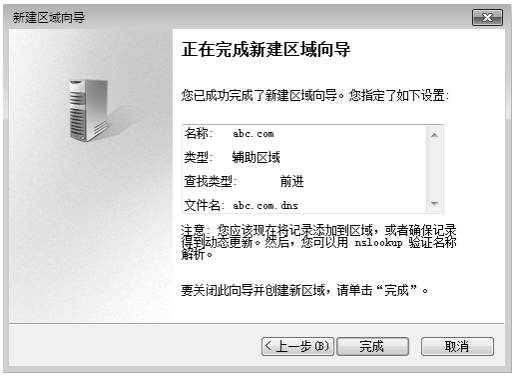


图 8-31　完成区域创建

8.4.3　子域和委派

1. 子域

在 DNS 区域中可以通过创建子域来扩展域名空间，例如，在区域“abc.com”中创建子域“bj.abc.com”，用来表示北京分公司的域名信息。子域的所有记录保存在上级（即创建子域的域）区域文件中，例如，子域“bj.abc.com”的信息保存在“abc.com.dns”文件中。

图 8-32　输入子域域名

要创建子域，可以右键单击需要新建子域的区域，在弹出的快捷菜单中选择“新建域”命令，出现“新建 DNS 域”对话框。在文本框中输入新建的 DNS 域名，即子域域名，如图 8-32 所示。单击“确定”按钮。创建子域后，就可以在子域中创建主机记录、指针记录、别名记录。

2. 委派

子域的信息都存储在父区域文件中，当区域中的子域过多时，维护起来很不方便，并且还会遇到域名查询量的瓶颈。通过在区域中新建委派，可以将子域委派到其他服务器。例如，根域 DNS 服务器和顶级域 DNS 服务器之间的关系就是委派，根域 DNS 将所有顶级域都委派出去，并且不接受递归查询，以降低自己的访问负荷和维护成本。

创建子域和创建委派操作都会创建一个新的域，但二者的区别是：在创建子域时，子域的权威服务器就是父区域中的权威服务器；而在创建委派时，要给新域指定权威服务器。

ABC 公司有一台 DNS 服务器，其内部局域网使用 abc.com 作为域名。现在，该公司在上海成立分公司，上海分公司使用专线和总公司连接。上海分公司计划使用 sh.abc.com 作为域名并且在本地进行解析。

在 Windows Server 2008 R2 系统通过委派方式建立子域的步骤如下所述。

STEP1　在上海分公司的 DNS 服务器上创建正向主要查找区域 sh.abc.com 及主机记录（www.sh.abc.com 域名主机地址为 192.168.1.20），如图 8-33 所示。

图 8-33　添加主机记录

STEP2 在父域的 DNS 服务器上添加主机记录，该主机记录的 IP 地址为子域所在的 DNS 服务器地址（位于上海的那台 DNS 服务器域名为 SHDNSSrv.abc.com，IP 地址为 192.168.1.10），如图 8-34 所示。

图 8-34　添加主机记录

STEP3 右键单击父域，选择“新建委派”命令，如图 8-35 所示。

图 8-35　新建委派

STEP4 在“新建委派向导”窗口中单击“下一步”按钮，输入要委派的子域名称，如图 8-36 所示，单击“下一步”按钮。

图 8-36　输入委派域的域名

STEP5 在“名称服务器”页面单击“添加”按钮，以便指定可以主持委派域的 DNS 服务器，如图 8-37 所示。

图 8-37　添加名称服务器

STEP6 在“新建名称服务器记录”页面输入上海的 DNS 服务器域名，单击“解析”按钮，解析成功后会自动添加该服务器的 IP 地址，单击“确定”按钮，如图 8-38 所示。

图 8-38　建立子域 DNS 的名称服务器记录

STEP7 添加完成后在“名称服务器”窗口会出现受委派域 DNS 的域名和 IP 地址，如图 8-39 所示。单击“下一步”按钮，按向导提示单击“完成”按钮，完成新建委派向导。

图 8-39　指定名称服务器

STEP8 在父域下出现的“sh”就是委派的子域，如图 8-40 所示。其中只有一条“名称服务器（NS）”记录，它记录着 sh.abc.com 的授权服务器 SHDNSSrv.abc.com。当父域 DNS 服务器收到查询 sh.abc.com 内的记录请求时，它会向 SHDNSSrv.abc.com 查询。

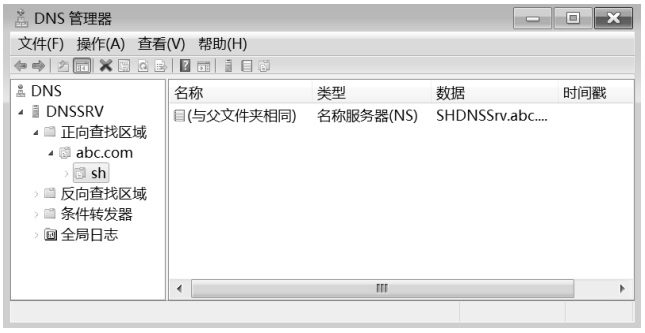


图 8-40　委派和子域

STEP9 在客户端上利用 Ping www.sh.abc.com 进行测试，它会向父域查询，父域会向委派的域查询。如图 8-41 所示，已成功解析 www.sh.abc.com 域名主机为 192.168.1.20。

图 8-41　检查域名解析

8.4.4　根提示

根提示使非根域的 DNS 服务器可以查找到根域的 DNS 服务器，根域 DNS 服务器分布在世界各地，为了定位这些根域 DNS 服务器，需要在非根域 DNS 服务器上配置根提示。

在 DNS 管理控制台窗口右键单击 DNS 服务器，从弹出的快捷菜单中选择“属性”，在其属性对话框中选择“根提示”选项卡，在“名称服务器”列表中共有 13 个根服务器，如图 8-42 所示。根服务器不要轻易修改，一般保持默认配置。如果 DNS 服务器配置了转发器，则优先查询转发器。

图 8-42　根提示

8.5　实训

实训环境一

HT 公司的局域网内没有 DNS 服务器，所有计算机都使用 ISP 的 DNS 服务器（202.97.224.28）。HT 公司计划搭建一台 DNS 服务器，为公司内部创建一个 huatian.com 区域，并为公司的服务器建立主机记录，使用户能用 FQDN（www.huatina.com）访问这些服务器，同时该 DNS 服务器能为内网用户解析公网域名。

需求描述

- 添加 DNS 角色服务，搭建 DNS 服务器。
- 创建区域，添加主机记录，实现局域网内部的域名解析。
- 设置转发器，使其指向公网 DNS 服务器，实现公网域名的解析。

实训环境二

HT 公司注册了一个域名 huatian.com。公司使用一台 DNS 服务器独立维护该域名，服务器的 IP 地址为 192.168.0.X。计划为北京分公司建立一个域名为 bj.huatian.com 的子域，并且

使用北京分公司的本地 DNS 服务器（IP 地址为 192.168.0.Y）来维护该子域，如图 8-43 所示。

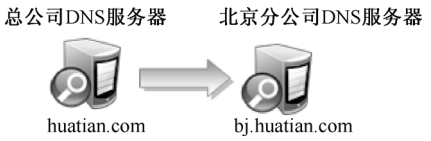


图 8-43　实训环境二示意图

需求描述

- 搭建第二台 DNS 服务器，放置在北京分公司。
- 在第二台 DNS 服务器上创建区域名为 bj.huatian.com 的主要区域。
- 在第一台 DNS 服务器上创建委派，委派的域名为 bj.huatian.com，主持该委派域的 DNS 服务器是第二台 DNS 服务器。

8.6　习题

- 域名空间结构有哪几层？
- DNS 查询有哪几种类型？分别适合什么情况？
- DNS 服务器要具备哪些条件？
- 常用的资源记录有哪些？具有什么作用？
- 查找资料，了解 nslookup 和 ipconfig/flushdns 命令的作用。

第 9 章

搭建 Web 和 FTP 站点

项目需求：

ABC 公司建立了自己的公司网站，网站地址为 www.abc.com，要搭建一台 Web 服务器来运行公司网站，为企业内部和互联网用户提供浏览服务。为了方便局域网内文件的上传和下载，还需要配置 FTP 服务器，并且设置上传和下载文件的权限。

技能目标：

- 了解 IIS 的主要功能
- 学会安装和配置 Web 站点
- 学会增强网站安全的配置方法
- 理解 FTP 的主要功能
- 掌握 FTP 站点的基本配置
- 掌握 FTP 站点的访问方式

MEMO

9.1 知识介绍——IIS 与 WWW 服务概述

Internet 为用户提供多种形式的海量信息，用户通过浏览 Web 站点，可以搜索自己所需的资料、图片和视频，所有这些都是基于 WWW（World Wide Web）服务实现的，WWW 服务也称为 Web 服务、万维网服务，是指在网上发布并可以通过浏览器观看的图形化页面服务。万维网服务是通过建立 Web 站点来实现的，目前应用较多的软件主要有 Apache 和 IIS（Internet Information Service）。

Apache 是一款开源软件，可以免费下载使用，支持 UNIX、Linux 和 Windows 等操作系统，具有配置简单、高效、性能稳定等特点。

IIS 是微软公司的 Web 服务器产品，它提供了图形化界面的管理工具，称为 Internet 服务管理器，用于配置和管理 Internet 服务。在 IIS 中包含了 Web 服务和 FTP 服务，分别用于浏览网页和传输文件，通过 IIS 使得在 Internet 或 Intranet 中实现信息互动成为一件很容易的事。

微软的 Internet 信息服务（IIS）提供了可用于 Intranet 和 Internet 或 Extranet 上的集成 Web 服务器能力，这种服务器具有可靠性、可扩展性、安全性等特点。任何规模的组织都可以使用 IIS 管理 Intranet 或 Internet 上的网页及文件传输（FTP）站点，IIS7.5 是 Windows Server 2008 R2 的 Web 服务器角色。

9.2 任务 1：安装和配置 Web 站点

ABC 公司为了方便开展线上业务，扩大公司的影响力，建立了公司网站作为网上订单、新闻发布、产品展示的平台，网站域名为 www.abc.com，为网站搭建 Web 服务器，步骤如下。

9.2.1 安装 IIS

Windows Server 2008 R2 在默认情况下并不安装 IIS，需要添加该服务器角色才能安装。

STEP1 打开“开始”→“管理工具”→“服务器管理器”窗口，选择“角色”，单击右侧的“添加角色”，单击“下一步”按钮。在“选择服务器角色”页面中选中“Web 服务器（IIS）”角色，并在弹出的对话框中单击“添加必需的功能”，如图 9-1 所示。

图 9-1 添加角色

STEP2 在“Web 服务器（IIS）简介”页面，单击“下一步”按钮，在“选择角色服务”页面不做修改，采用默认配置，单击“下一步”按钮。如果需要运行动态页面和提供 FTP 等，可以在这里选择相应的选项，如图 9-2 所示。

图 9-2　选择角色服务

STEP3 在“确认安装选择”页面确认选项无误后单击“安装”。当出现“安装结果”界面后，单击“关闭”按钮，完成 IIS 的安装。

STEP4 在安装 IIS 角色时会自动创建一个默认站点，可以使用服务器的 IP 地址访问该默认站点，以验证 IIS 的安装是否正常，如图 9-3 所示。

图 9-3　IIS 的默认站点

9.2.2 配置网站

添加 IIS 服务器角色后，可以使用“Internet 信息服务（IIS）管理器”来配置网站。从“管理工具”中打开“Internet 信息服务（IIS）管理器”，展开左侧节点，出现默认站点（Default Web Site），如图 9-4 所示。可以利用默认站点作为网站，也可以另外创建一个新网站。

图 9-4 默认站点

1. 配置站点的 IP 地址和 TCP 端口

要建立一个 Web 站点，首先要配置网站的 IP 地址和 TCP 端口。

STEP1 单击目标站点，选择右边“操作”窗格的“绑定”，在“网站绑定”窗口中选择当前的绑定方案，如图 9-5 所示，单击“编辑”按钮。

图 9-5 编辑默认绑定

STEP2 在“编辑网站绑定”窗口中， IP 地址为“全部未分配”，表示此站点将响应该计算机上没有分配给其他站点的所有 IP 地址，如图 9-6 所示，选择站点使用的 IP 地址。IP 地址中显示本机的 IP 地址为 192.168.1.1，本例中选择“全部未分配”或 192.168.1.1 均可。

“端口”80 表示 TCP 端口号，TCP80 端口是 Web 服务的默认端口。对于使用默认 80 端口的网站，用户在浏览器中输入“http://IP 地址（域名）”就可以访问该网站。如果修改了网站的 TCP 端口，则用户在浏览器中输入“http://IP 地址（域名）：端口号”才能访问网站。

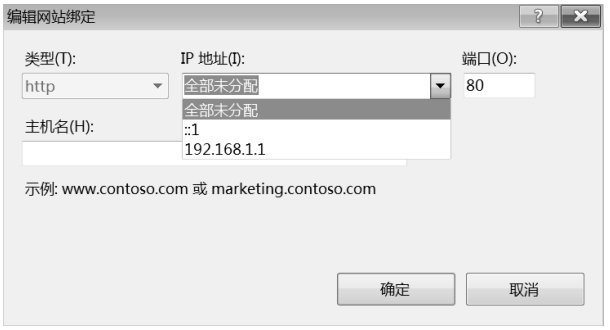


图 9-6　选择站点使用的 IP 地址

图 9-6 所示的“编辑网站绑定”对话框中还有“类型”和“主机名”项，绑定类型有“http”和“https”两类。HTTP（Hypertext Transfer Protocol）是超文本传输协议，用于在客户机和服务器之间以明文方式交互信息；HTTPS（Secure Hypertext Transfer Protocol）是安全超文本传输协议，使用 SSL 加密客户机和服务器之间的交互信息。

2．配置站点的物理路径和连接限制

站点的物理路径就是存放该站点页面文件的本地路径或远程路径，默认站点的默认路径为“%SystemDrive%\inetpub\wwwroot”，其中“%SystemDrive%”是 Windows Server 2008 R2 系统所在的盘符。出于安全方面的考虑，站点的物理路径应该与系统处于不同的磁盘分区。

连接限制通过连接超时、最大并发数和最大带宽三个方面限制站点的网络连接。

- 连接超时：设置服务器在断开与非活动用户的连接之前的等待时间，默认为 102 秒。
- 最大并发连接数：限制站点可以接受的最大并发连接数，防止系统负荷过重。
- 最大带宽：限制站点使用的网络带宽，防止 Web 服务占用过多网络带宽，从而影响其他网络服务。

单击目标站点，选择右边“操作”窗格的“高级设置”，出现如图 9-7 所示的“高级设置”对话框，在此话框中设置站点的物理路径、连接超时、最大并发连接数和最大带宽等。

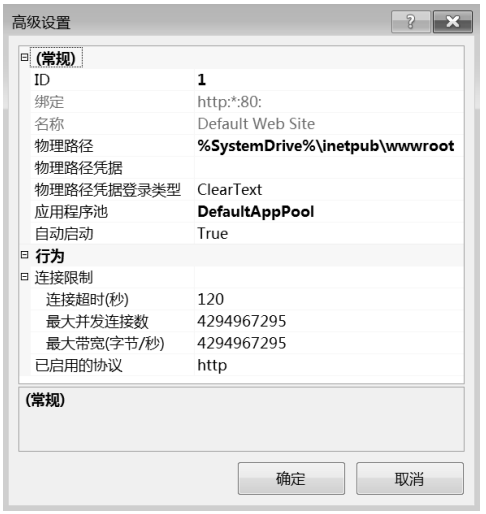


图 9-7　“高级设置”对话框

3．配置默认文档

当用户访问一个 Web 站点时，通常只使用域名或 IP 地址就可以访问，并不需要提供页面文件的名称，由于站点设置了默认文档，所以此网站会自动将主目录中的首页发送给用户。

用户可以设置站点的默认文档，选择目标站点，在中间窗格双击“默认文档”，如图 9-8 所示。

图 9-8 “默认文档”的位置

系统已经设置几个默认文档，如 Default.htm、Default.asp、index.htm、index.html 和 iisstart.htm，如图 9-9 所示。这些文件按从上到下的顺序优先显示，即当用户访问网站时，先检查站点的物理路径内有没有 Default.htm 文件，有则显示该文件，没有则检查第二个文件，依次类推。如果物理路径内没有默认文档，而用户又没有自行添加指定请求的文件，则用户会得到一个错误提示。

通过单击图 9-9 右侧窗格内的“添加”、“删除”、“上移”和“下移”按钮，用户可以添加新的默认文档，也可以调整现有文档的使用顺序，或者删除不用的默认文档。

图 9-9 默认文档

9.3　任务 2：配置虚拟目录和虚拟主机

9.3.1　配置虚拟目录

在站点的物理路径下可以有多个子文件夹，分别存放不同内容的文件。例如，在一个网站中，新闻类的网页文件存放在主目录中名为 news 的文件夹内，产品介绍类的网页文件存放在名为 products 的文件夹内。如果文件很多，主目录的空间可能有限。因此，需要将上述文件存放在其他分区或其他计算机上，而用户访问的上述文件夹在逻辑上还归属于网站，这种归属于网络之下的目录称为虚拟目录。

利用虚拟目录可以将一个网站的文件分散存储在同一台计算机的不同路径或其他计算机中（共享文件夹），使用虚拟目录有以下优点：

- 将数据分散保存到不同磁盘或计算机上，便于分别开发与维护。
- 当数据移动到其他物理位置时，不影响 Web 站点的逻辑结构。

创建虚拟目录可以通过以下步骤完成。

STEP1　打开“Internet 信息服务（IIS）管理器”，在左侧窗格右键单击目标站点，选择“添加虚拟目录”，如图 9-10 所示。

图 9-10　添加虚拟目录

STEP2　在“添加虚拟目录”对话框中，输入虚拟目录的名称和对应的物理路径，单击“确定”按钮，如图 9-11 所示。

STEP3　创建完成的虚拟目录会以节点的形式显示在站点下面，用户可以使用“http://域名（IP）/虚拟目录别名”来访问虚拟目录下的文件，如图 9-12 所示。

创建完虚拟目录后，可以修改其物理路径。在“Internet 信息服务（IIS）管理器”窗口选中虚拟目录，选择右侧操作窗格中的“基本设置”，在“编辑虚拟目录”对话框中可以重设物理路径，但不能更改虚拟目录的别名，如图 9-13 所示。在虚拟目录下也可以设置默认文

档，方法与配置站点的默认文档相同。

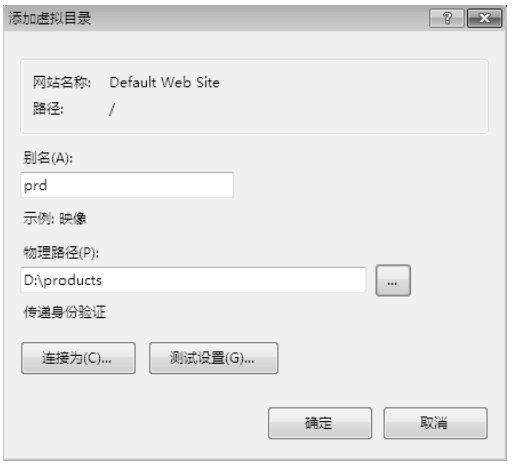


图 9-11　设置虚拟目录的别名和物理路径

图 9-12　访问虚拟目录

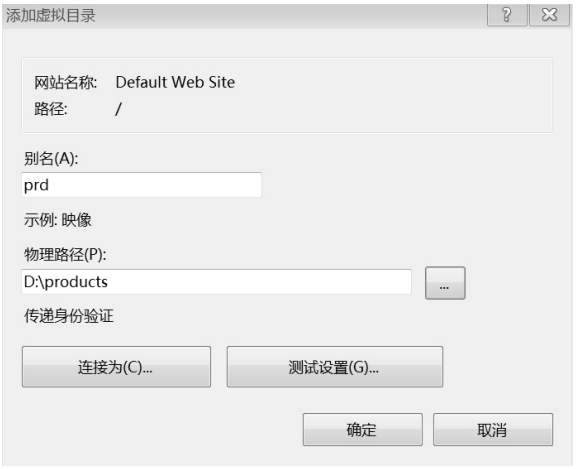


图 9-13　修改虚拟目录物理路径

9.3.2　配置虚拟主机

为了提高硬件资源的利用率，可以在一台服务器上运行多个网站，这些网站称为虚拟主机。实现虚拟主机一般有以下 3 种方式。

- 使用不同的 IP 地址。
- 使用相同的 IP 地址，不同的 TCP 端口号。
- 使用相同的 IP 地址和 TCP 端口号，不同的主机名。

1．使用不同的 IP 地址搭建多个 Web 站点

TCP/IP 协议规定，一个 IP 地址只能有一个 TCP80 号端口。如果在一台服务器上运行多个使用 80 端口的 Web 站点，则该服务器必须具有多个 IP 地址。使用不同 IP 地址搭建多个

Web 站点的步骤如下所述。

STEP1 在服务器本地连接的属性对话框中，选择“高级”按钮，出现如图 9-14 所示的“高级 TCP/IP 设置”对话框，单击“添加”按钮，添加新的 IP 地址。

图 9-14　高级 TCP/IP 设置

STEP2 打开“Internet 信息服务（IIS）管理器”，右键单击左侧窗格中的“网站”，选择“添加网站”，如图 9-15 所示。

图 9-15　添加网站

STEP3 在“添加网站”对话框中输入站点名称和物理路径，并选择该站点要使用的 IP 地址，单击“确定”按钮，如图 9-16 所示，配置新建网站。

STEP4 为新添加的站点准备一个默认页面文件，访问新站点，测试结果如图 9-17 所示。

图 9-16　配置新建网站

图 9-17　访问新站点

2．使用相同 IP 地址、不同 TCP 端口搭建多个 Web 站点

如果 Web 服务器上只有一个 IP 地址，但是需要搭建两个 Web 站点，这时可以让一个站点使用非 80 端口。当访问非 80 端口的站点时需要注明该站点的端口号，格式为“http://域名（IP）:端口”；如果不注明端口，则将尝试访问端口为 80 的网站。

STEP1　打开“Internet 信息服务（IIS）管理器”，右键单击左侧窗格的“网站”，选择“添加网站”。在“添加网站”对话框中输入站点名称和物理路径，并选择该站点要使用的 IP 地址和端口号，单击“确定”按钮，如图 9-18 所示，配置不同端口号。

STEP2　为该站点准备一个默认页面文件，使用端口号访问站点，测试结果如图 9-19 所示。

注意：

如果在一台服务器上创建的两个站点使用相同的 IP 和端口号，则其中会有一个站点不能启动。

图 9-18　配置不同端口号

图 9-19　使用端口号访问站点

3．使用相同 IP 地址和 TCP 端口，不同的主机名搭建多个 Web 站点

虽然使用相同 IP 和不同的端口号可以搭建多个 Web 站点，但是非 80 端口不便于用户访问，用户在访问网站时必须知道站点的端口号。另外，在输入 URL 时，还必须输入端口号，访问时非常不方便。如果使用不同的 IP 地址搭建多个站点，为每个站点申请一个 IP 地址显然有些浪费，针对上述问题，可以使用相同的 IP 地址和 TCP 端口、不同的主机名来搭建多个站点。

主机名就是与站点对应的 FQDN（完全合格的域名）。使用主机名搭建 Web 站点后，Web 服务器将根据用户请求访问的 FQDN 判断用户要访问的站点，不再受 IP 地址或端口号的限制。

STEP1　在 DNS 服务器上为站点注册一个主机记录，例如，FQDN 是 www.abc.com，IP 地址是 192.168.1.1，如图 9-20 所示。

STEP2　打开“Internet 信息服务（IIS）管理器”，在“添加网站”窗口中，输入站点名称和物理路径，并选择该站点要使用的 IP 地址、端口号和主机名，单击“确定”按钮，如图 9-21 所示。

STEP3　为该站点准备一个默认页面文件，使用 FQDN“www.acb.com”访问，如图 9-22 所示。

图 9-20　注册主机记录

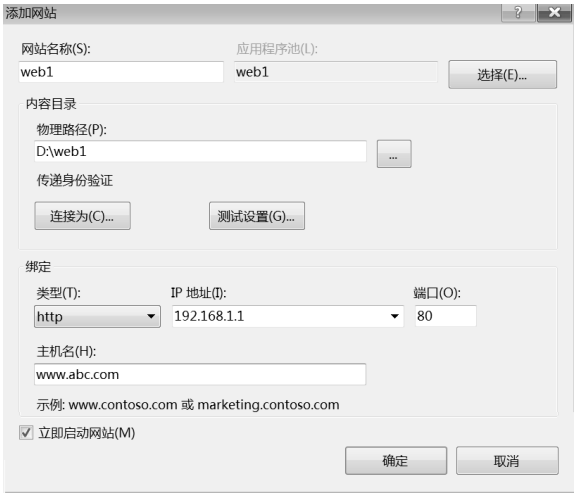


图 9-21　建立有主机名的新站点

图 9-22　使用 FQDN 访问站点

9.4　任务 3：保证站点的安全

Web 站点建成后，就可以对用户提供信息浏览服务，通常是允许匿名访问的；但有些特殊网站或虚拟目录出于安全性考虑，要求用户提供用户账户和密码后才能访问，或者限定某些 IP 地址访问。

在 IIS7.5 下要更好地实现站点的安全性，需要为 Web 服务器角色添加所需的角色服务，这些角色服务在安装 Web 服务器角色时默认是不安装的。选择“开始”→“管理工具”→“服务器管理器”→“角色”，在“服务器管理器”窗口单击“Web 服务器（IIS）”，如图 9-23 所示。单击“添加角色服务”，在如图 9-24 所示“选择角色服务”页面，选择需要添加的安全性角色，单击“下一步”按钮。

图 9-23　Web 服务器（IIS）角色

图 9-24　安全性角色服务

9.4.1　身份验证和访问控制

常见的身份验证方法如下所述。

- 匿名身份验证：系统默认只启用匿名身份验证。启用匿名身份验证后用户无须输入用户名和密码，当用户试图连接到网站时，Web 服务器将连接分配给账户 IUSR，用户实际上是使用 IUSR 这个账户访问站点的。
- Windows 身份验证：Windows 身份验证也会要求输入用户名与密码，而且用户名与密码在通过网络发送之前会经过哈希处理，因此可以确保安全性。Windows 使用 NTLM 或 Kerberos 协议对客户端进行身份验证，由于 Kerberos 会被防火墙阻挡且代理服务器不支持 NTLM，所以 Windows 身份验证适用于连接内部网络（Intranet）的网站。
- 基本身份验证：基本身份验证要求用户提供有效的用户名和密码才能访问，它是工业标准验证方法；但是用户发送给网站的用户名和密码并没有被加密，所以容易被恶意拦截并得知这些数据。若要使用基本身份验证，应该搭配其他可以确保发送数

据安全性的措施。

- 摘要式身份验证：摘要式身份验证也要求输入用户名和密码，它比基本身份验证更安全。在使用摘要式身份验证时，密码不是以明文形式发送的。与 Windows 身份验证相比，摘要式身份验证可以通过代理服务器使用。

禁用匿名访问的步骤如下所述。

STEP1 打开“Internet 信息服务（IIS）管理器”，在左侧窗格中选择目标站点或虚拟目录，在中间窗格中双击“身份验证”，如图 9-25 所示设置身份验证。

图 9-25　设置身份验证

STEP2 在打开的“身份验证”窗格中，选择“匿名身份验证”，在右侧的“操作”窗格中单击“禁用”，如图 9-26 所示。设置完成后，用户访问该站点时将被要求提供用户名和密码。

图 9-26　禁用匿名身份验证

注意：

必须确保站点至少启用了一种身份验证方式，否则所有用户都将无法访问该站点。只有域内的成员计算机才可以启用摘要式身份验证。

9.4.2　IP 地址和域名限制

Web 站点可以授权或者拒绝一台或者一组客户机访问，禁用一组 IP 地址访问的步骤如下所述。

STEP1 打开“Internet 信息服务（IIS）管理器”，在左侧窗格中选择目标站点或虚拟目录，在中间窗格中双击“IPv4 地址和域限制”，如图 9-27 所示。

图 9-27　IPv4 地址和域限制

STEP2 在打开的“IP 地址和域限制”窗格中，单击“添加拒绝条目”，如图 9-28 所示。

图 9-28　添加拒绝条目

STEP3 在“添加拒绝限制规则”对话框中，输入想要拒绝的 IP 地址或 IP 地址范围，单击“确定”按钮，如图 9-29 所示。

STEP4 添加完成后，192.168.8.0/24 网段的用户将无法访问该站点，禁止访问提示如图 9-30 所示。

图 9-29　添加拒绝限制规则

图 9-30　禁止访问提示

如果要通过域名允许或拒绝访问，需要编辑功能设置，单击图 9-28 中的“编辑功能设置”，在打开的“编辑 IP 和域限制设置”对话框中勾选“启用域名限制”，如图 9-31 所示。启用域名限制会严重影响服务器性能，建议不启用。

9.4.3　NTFS 权限

网页文件一般存储在 NTFS 磁盘分区中，以便利用 NTFS 权限来增加网页的安全性。当客户机访问网站时，服务器会经过一系列检查以确定该客户是否能访问此站点。首先服务器会检查客户机的 IP 地址是否被授权，然后检查用户账户和密码是否正确，接着检查用户账户或匿名账户是否被授予了访问权限，如果没有访问权限，客户端将会显示如图 9-30 所示的提示信息，最后检查网站文件的 NTFS 权限，如果用户使用的账户对网站文件没有 NTFS 读取权限，客户端将会显示如图 9-32 所示的窗口。

图 9-31　启用域名限制

图 9-32　没有站点目录的 NTFS 读取权限

9.4.4　启用日志

如果网站启用日志记录，管理员可以通过查看日志跟踪网站被访问的情况，如哪些用户访问了本站点，访问者查看了什么内容，以及最后一次查看信息的时间等。可以使用日志来评估内容受关注程度或识别信息的瓶颈。有时还可以通过日志查出有哪些非授权用户访问网站，以便采取应对措施。日志默认存储在“%SystemDrive%\inetpub\logs\LogFiles”中。

打开“Internet 信息服务（IIS）管理器”，在左侧窗格中选择目标站点或虚拟目录，在中

间窗格中双击“日志”，打开日志窗格，如图 9-33 所示。

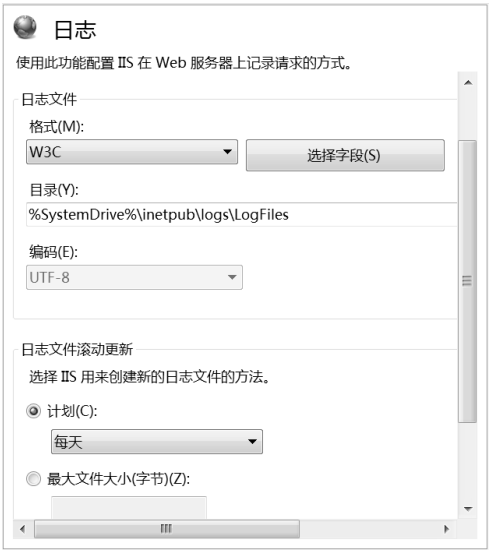


图 9-33　日志窗格

在打开的“日志”窗格中，可以看到日志的格式、日志文件产生的时间间隔和存放的位置。可以保持默认设置，即采用 W3C 格式，每天产生一个日志文件。

9.5　任务 4：安装和配置 FTP 服务

FTP（File Transfer Protocol）是一个用来在两台计算机之间传送文件的通信协议，它建立在传输层 TCP 协议之上，利用它可以给用户提供文件上传和下载服务。FTP 服务器是在互联网或局域网中提供 FTP 服务的计算机，它可以是专用服务器，也可以是个人计算机。启动 FTP 服务后，用户可以连接到服务器下载文件；如果权限允许，用户也可以把文件上传到 FTP 服务器。

ABC 公司文件服务器存储了大量业务文档，通过文件共享在局域网内提供下载服务，异地的公司员工也需要从文件服务器下载资料或上传数据到文件服务器，文件共享已无法满足需求，需要搭建 FTP 服务器来实现，FTP 服务器还可以通过访问权限的设置保证数据来源的正确性和数据存取的安全性。

9.5.1　安装 FTP 服务

Windows 系统中的 FTP 服务是基于 IIS 服务创建的，默认在安装 Web 服务器角色时并不安装 FTP 服务，在 Windows Server 2008 R2 系统安装 FTP 服务的步骤如下所述。

STEP1　打开“开始”→“管理工具”→“服务器管理器”窗口，选择“Web 服务器（IIS）”，单击“添加角色服务”，在“选择角色服务”页面勾选“FTP 服务器”项，单击“下一步”按钮，如图 9-34 所示。

图 9-34　添加 FTP 角色服务

STEP2 依据提示安装 FTP 服务，安装成功后，出现如图 9-35 所示页面，单击“关闭”按钮，完成安装。

图 9-35　完成安装

9.5.2　添加 FTP 站点

STEP1 打开“Internet 信息服务（IIS）管理器”，右键单击左侧窗格中的“网站”，选择“添加 FTP 站点”或者选择右侧“操作”窗格中的“添加 FTP 站点”，如图 9-36 所示。

STEP2 在“站点信息”对话框中输入 FTP 站点名称和站点物理路径，单击“下一步”按钮，如图 9-37 所示。

STEP3 在“绑定和 SSL 设置”页面设置绑定的 IP 地址，其他设置保持默认，如图 9-38 所示，单击“下一步”按钮。

STEP4 在“身份验证和授权信息”页面设置身份验证方式为“匿名访问”，允许所有用户读取，如图 9-39 所示，单击“完成”按钮。如果允许用户写入，则用户可以上传文件到 FTP 服务器（结合 NTFS 权限设置写入权限）。

图 9-36　添加 FTP 站点

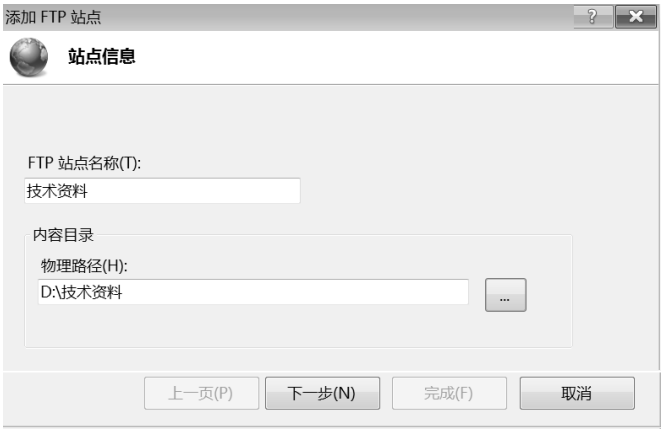


图 9-37　设置站点名称和物理路径

图 9-38　设置绑定 IP 地址

图 9-39　设置身份验证方式及用户权限

STEP5 为该 FTP 站点准备要下载的文件，浏览该 FTP 站点，用 Web 方式访问 FTP 站点测试结果如图 9-40 所示。

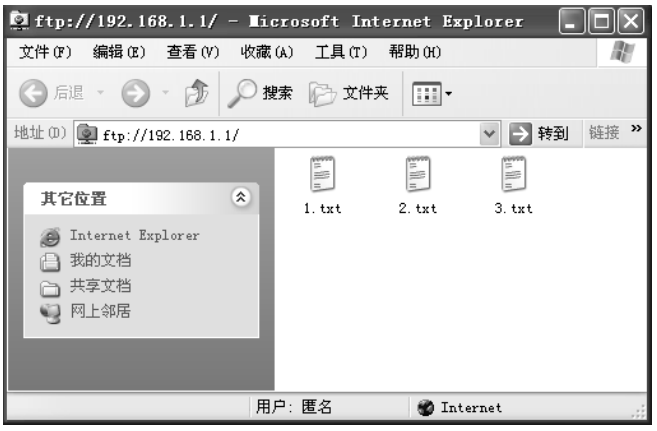


图 9-40　用 Web 方式访问 FTP 站点测试结果

9.5.3　FTP 站点的基本设置

对已经创建的 FTP 站点，可以进行目录列表样式、网站绑定、网站信息、验证设置、授权设置、查看当前连接的用户，以及通过 IP 地址与域名来限制连接等设置，这里的有些设置与 Web 网站设置相同，可以参照进行。

1．目录列表样式

用户在查看 FTP 网站中的文件时，界面上显示的文件列表格式有 MS-DOS 与 UNIX 两种，打开“Internet 信息服务（IIS）管理器”，选择“网站”下要设置目录样式的 FTP 站点，

在站点主页页面中双击“FTP 目录浏览”，如图 9-41 所示。在打开的目录浏览页面中会显示目录列表样式，如图 9-42 所示。

图 9-41　FTP 目录浏览

图 9-42　目录列表样式

注意:

如果用户使用 Internet Explorer 或 Windows 资源管理器来连接 FTP 站点，则界面中显示文件的方式不会受到目录列表样式设置的影响，只有使用命令行方式连接 FTP 站点时才会有所不同。

2．FTP 网站的信息设置

可以为 FTP 网站设置显示信息，用户在连接 FTP 网站时就会看到这些信息。选择要设置的 FTP 站点，双击图 9-41 中的“FTP 消息”，打开 FTP 站点的 FTP 消息页面，如图 9-43 所示。

图 9-43　FTP 消息

- 横幅：用户在连接 FTP 网站时，会先看到横幅处的文字。
- 欢迎使用：当用户登录到 FTP 网站时会看到的欢迎词。
- 退出：当用户退出时会看到的欢送词。
- 最大连接数：如果 FTP 网站有连接数量限制，而且当前的连接数目已经达到限制值，此时若用户连接 FTP 网站，将看到此处设置的信息。

注意：

如果用户使用 Internet Explorer 连接 FTP 站点，则不会显示 FTP 消息；如果使用 CuteFTP 或 SmartFTP 等软件来连接 FTP 站点，就可以显示 FTP 消息。

3．身份验证与权限设置

FTP 站点的身份验证设置与 Web 站点的身份验证设置相似，有匿名身份验证与基本身份验证两种。双击图 9-41 中的“FTP 授权规则”，打开 FTP 授权规则页面，可以设置用户访问权限，如图 9-44 所示，在创建 FTP 站点时已经设置为所有用户可以读取的权限。如果要更改这个权限，单击右侧操作窗格中的“编辑”，在“编辑允许授权规则”对话框中修改用户访问权限，还可以单击“添加允许（拒绝）规则”来添加新的规则。

图 9-44　FTP 授权规则

图 9-45　添加虚拟目录

9.5.4　配置虚拟目录

给 FTP 站点创建虚拟目录与给 Web 站点创建虚拟目录一样，虚拟目录的创建并不局限于把本地计算机中的目录添加到虚拟目录中，也可以把网络共享目录映射到虚拟目录中。右键单击 FTP 站点，从弹出的快捷菜单中选择“添加虚拟目录”，输入虚拟目录别名和物理路径，如图 9-45 所示，单击“确定”按钮完成虚拟目录创建。访问虚拟目录的方法是在浏览器中输入“ftp：//FTP 站点 IP（域名）/虚拟目录别名”。

9.6　任务 5：使用 FTP 客户端

FTP 客户端可以通过 FTP 命令、Internet Explorer 浏览器、Windows 资源管理器和客户端软件等方式来连接。

9.6.1　FTP 命令行

进入命令提示符状态后，输入“ftp FTP 站点 IP 或域名”，根据命令提示输入用户名和密码。如果使用匿名方式登录，在用户名“User”处输入“anonymous”，在密码“Password”处直接按回车键。结束与远程计算机的 FTP 会话并退出 FTP，输入“bye”命令，如图 9-46 所示。

图 9-46　登录与退出 FTP

在命令行模式下访问 FTP 站点，必须使用命令才能进行相应的操作。若要显示目录文件和子目录列表，则输入“dir”命令；若要更改远程计算机的工作目录，则输入“cd 目录名”命令；若要下载远程计算机上的文件，则输入“get 文件名”命令，如图 9-47 所示。如果要将本地当前目录的文件上传到 FTP 服务器的工作目录中，则输入“put 文件名”命令。一次下载多个文件使用“mget”命令，一次上传多个文件使用“mput”命令。

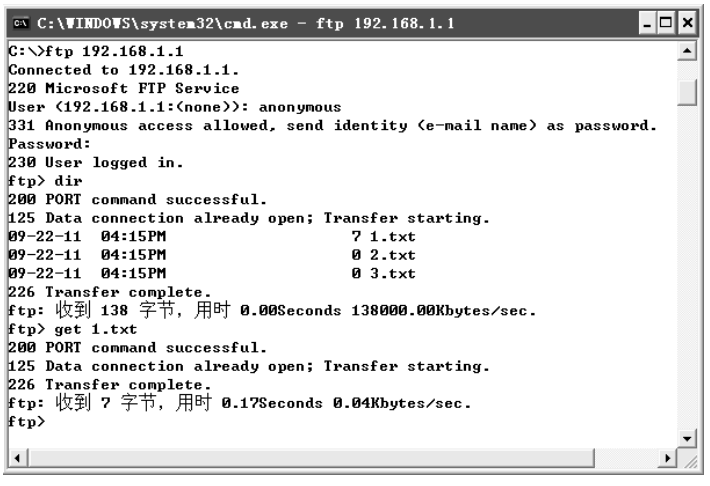


图 9-47　下载文件

9.6.2 Web 或资源管理器方式

用户可以在客户端通过浏览器或 Windows 资源管理器连接到 FTP 服务器。打开浏览器或 Windows 资源管理器，在“地址”处输入“ftp://FTP 站点 IP（域名）”，只要用户有相应的权限，就能进行文件的上传和下载。

9.7 实训

实训环境一

HT 公司在 ISP 托管了一台 Web 服务器，实训环境一示意图如图 9-48 所示，域名为 www.huatian.com。网站要求禁用匿名访问，网络管理员负责搭建此 Web 服务器。

图 9-48 实训环境一示意图

需求描述

- 添加 Web 角色服务，在安装过程中选择安装“安全性”角色。
- 创建新站点，不为站点指定具体的 IP 地址，使用默认的 80 端口，注明站点使用的主机名。
- 注册站点域名，并添加相应的主机记录。
- 禁用匿名身份验证，启用摘要式身份验证。

实训环境二

HT 公司需要在局域网中配置一台 FTP 服务器，实训环境二示意图如图 9-49 所示。该 FTP 服务器供内部员工下载和上传文件，但若用户不提供用户名和密码就不能登录。

图 9-49 实训环境二示意图

需求描述

- 安装 FTP 服务。
- 建立 FTP 站点。
- 设置站点访问权限。
- 使用 IE 浏览器访问 FTP 站点。

9.8　习题

- IIS 下的 Web 站点有几种身份验证方式？
- 在一台 IIS 服务器中同时运行多个 Web 站点有哪几种方式？
- FTP 客户端可以通过哪几种方式来连接 FTP 站点？
- 可以采用哪些方法保证 Web 站点的安全性？
- 当使用 FTP 命令行模式登录 FTP 服务器时，如何使用匿名方式登录？

第 10 章

远程访问服务（RAS）

项目需求：

ABC 公司业务延伸到多个省份，员工需要经常到外地出差，在出差期间需要访问位于公司内部网络的重要技术资料，为避免数据在传送途中被他人拦截，要求通过网络传送的数据文件要加密传送，同时要限制员工远程访问的时间。

技能目标：

- 理解远程访问服务的作用
- 会配置远程访问服务器
- 会配置客户机的网络连接
- 会配置网络策略控制访问

MEMO

10.1 知识介绍——远程访问概述

远程访问服务（Remote Access Service，RAS）是指客户机通过拨号连接或虚拟专用连接登录网络。客户机一旦得到 RAS 服务器的确认，就可以通过远程访问方式与公司内部网络建立连接，以便访问公司内部资源。远程访问适用于分公司或出差员工需要访问公司网络资源，Windows Server 2008 R2 的远程访问服务提供了两种连接方式，远程访问示意图如图 10-1 所示。

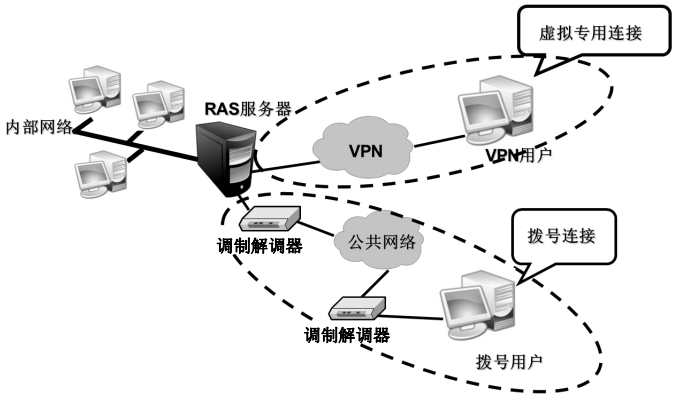


图 10-1 远程访问示意图

1．拨号网络

通过使用电信供应商提供的服务，如电话、ISDN、X.25 等，远程客户端使用非长久的拨号连接到 RAS 服务器的物理端口上，此时使用的网络为拨号网络。拨号网络需要在客户端安装调制解调器，使用拨号网络拨打 RAS 服务器某个端口的电话号码。

2．虚拟专用网络

虚拟专用网络（Virtual Private Network，VPN）是穿越公共网络的安全的点对点连接。在虚拟专用网中，客户端使用特定的基于 TCP/IP 的隧道协议与服务器建立连接。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴、供应商等同公司内部网络建立可信的安全连接，保证数据的安全传输。

3．拨号网络的组件

拨号网络由客户端、RAS 服务器、WAN 基础结构、LAN 协议等网络要素组成。

- 拨号网络客户端：即远程访问客户端，Windows 系列的操作系统都可以作为拨号网络客户端与 Windows Server 2008 R2 远程访问服务器建立连接，客户端上需要安装拨号设备，如调制解调器。
- RAS 服务器：运行 Windows Server 2008 R2 远程访问服务，可以接收拨号连接，并且能与远程访问客户端之间传递数据。
- WAN 基础结构：通过远程访问客户端、RAS 服务器和 WAN 基础结构上安装的拨

号设备，可以建立不同类型的拨号连接。最常用的拨号远程访问包括公用电话交换网、综合业务数字网、非对称数字用户线路等。

- 远程访问协议：用来控制连接的建立、数据在 WAN 链路上的传输。远程访问客户端与 RAS 服务器所使用的操作系统与 LAN 协议决定了客户机所能使用的远程访问协议。Windows Server 2008 R2 远程访问支持点到点协议（Point to Point Protocol，PPP）、串行线路网际协议（Serial Line Internet Protocol，SLIP）、Microsoft RAS 协议。
- LAN 协议：远程访问客户端用来访问连接到 RAS 服务器上的网络资源而使用的协议。Windows Server 2008 R2 远程访问服务支持 TCP/IP、IPX 和 NetBEUI 等协议。

4．VPN 网络组件

VPN 基于公共网络，在两个或两个以上的局域网之间创建传输数据的网络隧道。当传输数据通过网络隧道时，进行安全的 VPN 数据加密，从而确保用户数据的安全性、完整性和真实性。要使用 VPN 远程访问，需将 RAS 服务器配置为 VPN 服务器。VPN 服务器和客户机通过 ISP（互联网服务提供商）在 Internet 上建立虚拟连接。

VPN 网络的组成要素如下所述。

- VPN 客户端：VPN 客户端可能是一台单独的计算机，也可能是一台路由器。一般，VPN 客户端需要通过当地 ISP 连接上公共网络，以便和 VPN 服务器连接。
- VPN 服务器：VPN 服务器是接受 VPN 客户端 VPN 连接的计算机，该计算机一般使用专线连接公共网络，具有固定的 IP 地址。
- 隧道：用于连接中封装数据的部分。
- VPN 连接：用于连接过程中加密数据的部分，对典型的安全 VPN 连接，数据会被加密和压缩。
- 隧道协议：用来管理隧道及压缩专用数据的协议。Windows Server 2008 R2 支持 PPTP（点对点隧道协议）、L2TP（第二层隧道协议）、SSTP（安全套接字隧道协议）等 VPN 协议。

在实际工作中 VPN 比拨号网络应用更普遍，所以本章以 VPN 技术为例来说明 Windows 远程访问服务的配置及应用。

10.2　任务 1：配置远程访问服务

ABC 公司技术部的小刘出差到上海，需要用到一份非常重要的技术资料，可是这份资料在公司内部的文件服务器内。为了确保资料的安全性，不能在互联网上通过邮箱传输。ABC 公司的网络管理员要配置远程访问服务器，使小刘通过 VPN 登录到企业内部的文件服务器下载技术资料。

10.2.1　搭建远程访问服务器

为实现出差员工远程访问，需要搭建一台专用的远程访问服务器，该服务器同时连接内网（Intranet）和 Internet，并且配置路由和远程访问服务功能。服务器的内网 IP 地址是

192.168.1.2，公网 IP 地址是 200.100.1.1/24，VPN 访问示意图如图 10-2 所示。

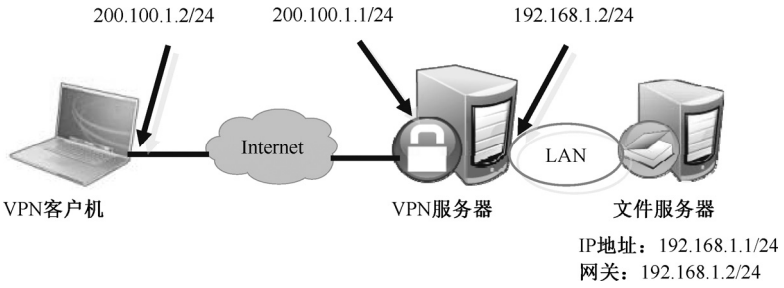


图 10-2　VPN 访问示意图

为 VPN 服务器添加网卡，两个网卡（名称分别为本地连接和公网连接）分别配置如图 10-2 所示的内网和外网 IP 地址。打开“服务器管理器”窗口，选择“角色”，单击“添加角色”，选择“网络策略和访问服务”角色，单击“下一步”按钮，如图 10-3 所示。在“选择角色服务”页面框选择“路由和远程访问服务”，根据提示完成角色添加，如图 10-4 所示。

图 10-3　添加网络策略和访问服务

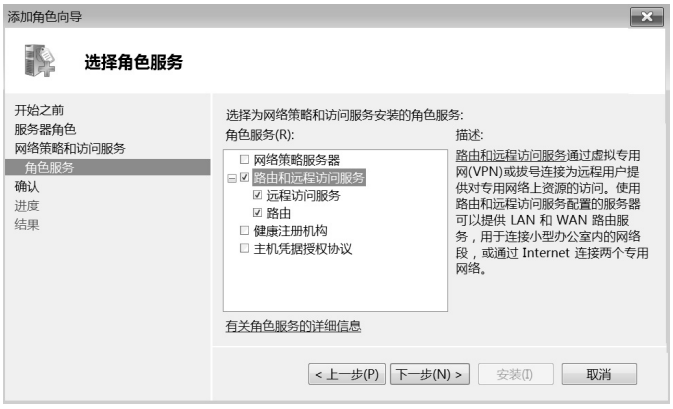


图 10-4　添加路由和远程访问服务

10.2.2　激活路由和远程访问服务

完成路由和远程访问服务配置后，其初始状态处于停用状态，需要激活后才能提供远程访问服务，具体步骤如下所述。

STEP1 选择“开始”→“管理工具”→“路由和远程访问”，打开“路由和远程访问”窗口。默认情况下服务器图标为红色下箭头，表明为停止状态。右键单击服务器名称，选择“配置并启用路由和远程访问”，如图 10-5 所示激活路由和远程访问服务。

图 10-5　激活路由和远程访问服务

STEP2 在“路由和远程访问服务器安装向导”页面单击“下一步”按钮，进入“配置”页面，选择“远程访问（拨号或 VPN）”，单击“下一步”按钮，配置远程访问服务，如图 10-6 所示。

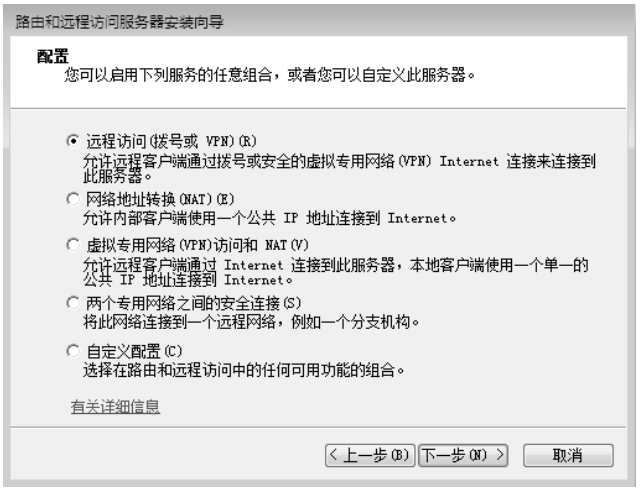


图 10-6　配置远程访问服务

STEP3 在“远程访问”页面选择“VPN”复选框 ，单击“下一步”按钮，如图 10-7 所示。

STEP4 在“VPN 连接”页面选择连接到 Internet 的网络接口，不勾选“通过设置静态数据

包筛选器来对选择的接口进行保护”，单击“下一步”按钮，如图 10-8 所示。

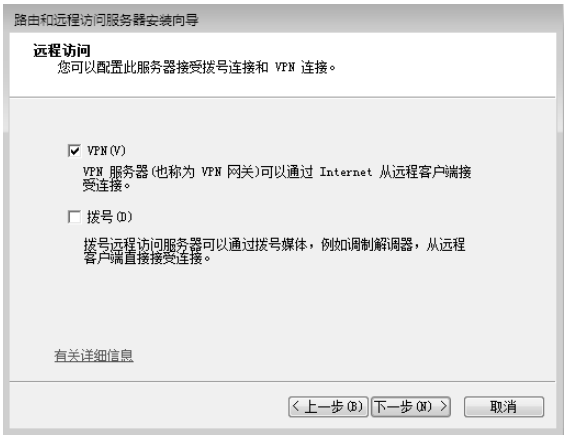


图 10-7　选择 VPN 连接

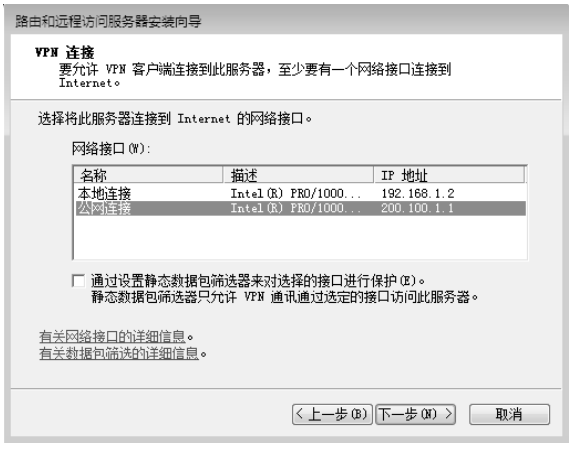


图 10-8　选择 Internet 网络接口

STEP5 在“IP 地址分配”页面选择“来自一个指定的地址范围”，单击“下一步”按钮，如图 10-9 所示。

图 10-9　选择分配 IP 地址的方法

注意：

如果在网络中有 DHCP 服务器，可以选择“自动”，让 DHCP 服务器自动为远程用户分配 IP 地址。

STEP6 在“地址范围分配”页面单击“新建”，输入计划分配给远程用户的局域网内部 IP 地址，单击“确定”按钮，返回到“地址范围分配”页面，如图 10-10 所示。单击“下一步”按钮。

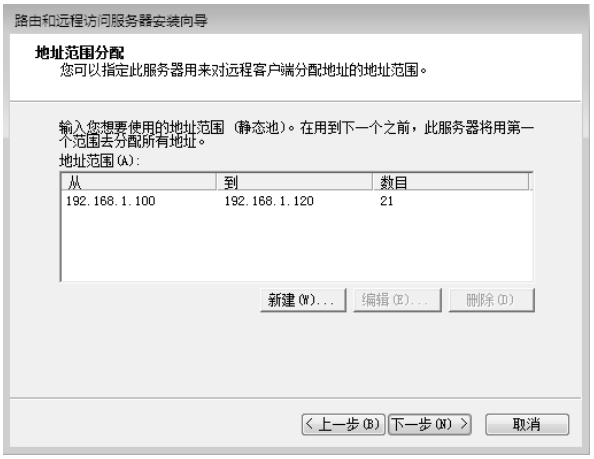


图 10-10　指定地址范围

STEP7 在“管理多个远程访问服务器”页面，选择“否，使用路由和远程访问来对连接请求进行身份验证”，不使用 RADIUS 服务器，如图 10-11 所示。单击“下一步”按钮。

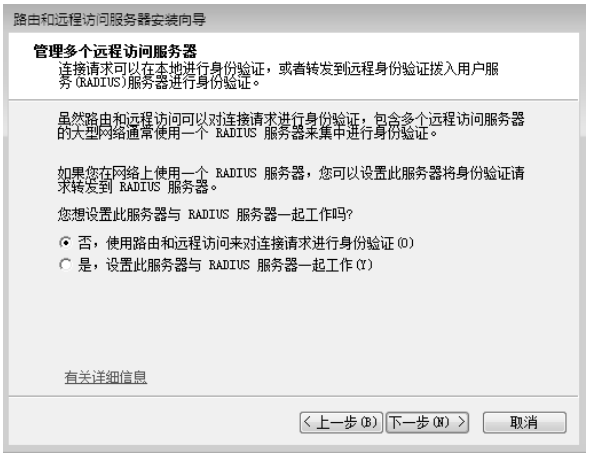


图 10-11　不使用 RADIUS 服务器

注意：

RADIUS 被称为远程验证拨入用户服务，使用 RADIUS 服务器可以集中管理所有的远程访问服务器，如进行验证、授权和计费等操作。

STEP8 单击“完成”按钮，会出现如图 10-12 所示的 DHCP 中继服务提示信息。由于安装

程序会顺便将 VPN 服务器设置为 DHCP 中继代理程序，所以会提醒在 VPN 服务器设置完成后，还需要在 DHCP 中继代理处指定 DHCP 服务器的 IP 地址，以便将索取 DHCP 选项设置的请求转给 DHCP 服务器。单击“确定”按钮。

图 10-12　DHCP 中继服务提示信息

STEP9 完成路由和远程访问服务器激活后，服务为启动状态，服务器图标变成绿色向上箭头，如图 10-13 所示启动路由和远程访问服务。

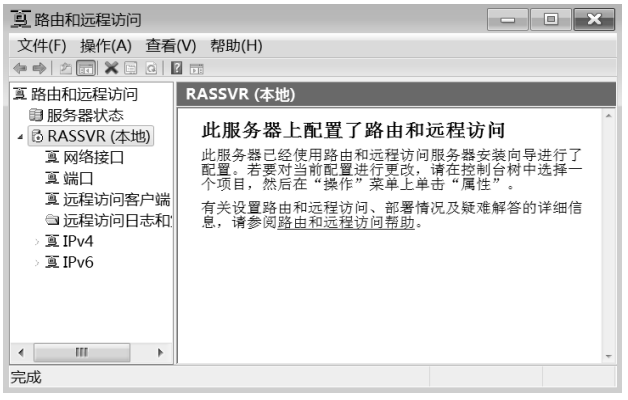


图 10-13　启动路由和远程访问服务

10.2.3　配置远程访问服务器

激活了路由和远程访问服务后可以为用户提供基本的服务，但在实际工作中，还需要修改路由和远程访问服务的配置，以实现更多的功能。

1．配置远程访问服务器的属性

在“路由和远程访问服务”窗口中，右键单击服务器名称，在弹出的快捷菜单中选择“属性”，可以对 RAS 服务器的属性进行配置，如图 10-14 所示。

（1）“常规”选项卡

“常规”选项卡中的信息与在安装过程中获得的信息完全相同，通过清除或选中路由器和远程访问服务器的复选框，可以改变服务器的角色，如图 10-15 所示。

（2）“安全”选项卡

“安全”选项卡中的信息允许管理员选择身份验证的协议和安全措施，单击“身份验证方法”按钮，可以配置服务器所使用的身份验证方法，如图 10-16 所示。

图 10-14　配置路由和远程访问的属性

图 10-15　“常规”选项卡

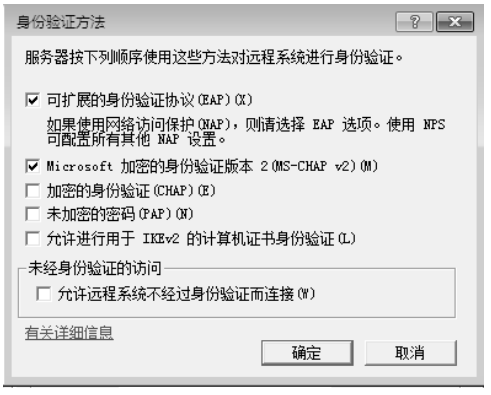


图 10-16　身份验证方法

（3）“IPv4”选项卡

在“IPv4”选项卡中可以为远程客户机动态分配或静态指派 IPv4 地址，如果允许远程客户访问远程服务器的整个局域网，则需要选择“启用 IPv4 转发”复选框；如果只允许远程客户访问该服务器，则清除此复选框，如图 10-17 所示。

如果远程访问服务器使用 IPv6 地址，则需要在“IPv6”选项卡中指定 IPv6 前缀。

（4）“PPP”选项卡

点对点协议（Point to Point Protocol，PPP）允许管理员设置连接时使用 PPP 选项。选择“多重链接”复选框，允许远程访问客户和请求拨号路由器将多个物理连接组合成单一的逻辑连接；选择“软件压缩”复选框，指定服务器使用 Microsoft 点对点压缩协议来压缩在远程访问连接时发送的数据，如图 10-18 所示。

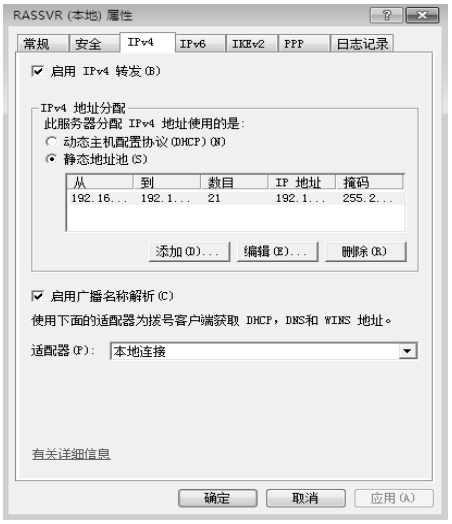


图 10-17 “IPv4”选项卡

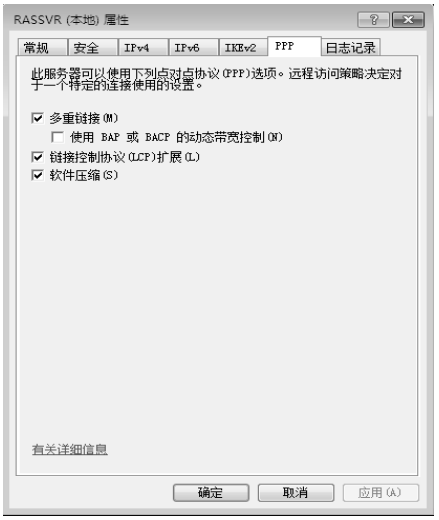


图 10-18 “PPP”选项卡

（5）“日志记录”选项卡

“日志记录”选项卡中提供了 4 个选项，用来配置所需的记录。使用“管理工具”→“事件查看器”可以打开日志信息，以便排除故障。

2．设备和端口

设备是为远程访问建立点对点连接提供可使用的端口的硬件和软件，设备可以是物理的或虚拟的，可以支持一个端口或多个端口。点对点隧道协议（PPTP）和第二层隧道协议（L2TP）就是虚拟多端口设备的示例，每个隧道协议都支持多个 VPN 连接。

如果要查看已安装的设备，可以在“路由和远程访问服务”窗口右键单击“端口”，选择“属性”，弹出“端口 属性”对话框，如图 10-19 所示。管理员可以更改设备的配置，在图 10-19 中选中需要配置的设备，单击“配置”按钮，在“配置设备”对话框进行配置，如图 10-20 所示。

图 10-19 端口属性

图 10-20 配置设备

还可以在“路由和远程访问服务”窗口单击“端口”查看拨号端口。路由和远程访问中的端口如图 10-21 所示。

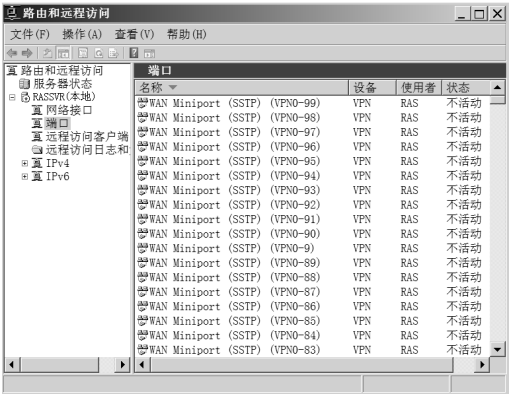


图 10-21　路由和远程访问中的端口

3．配置用户远程访问权限

独立服务器或域控制器管理的用户对象属性中都包含拨入属性，拨入属性允许或禁止用户连接到远程访问服务器，对于远程访问用户，需要赋予远程访问权限。

打开“Active Directory 用户和计算机”窗口，右键单击需要远程访问的用户账户，选择“属性”，在“属性”对话框中单击“拨入”选项卡，选择“允许访问”，如图 10-22 所示。

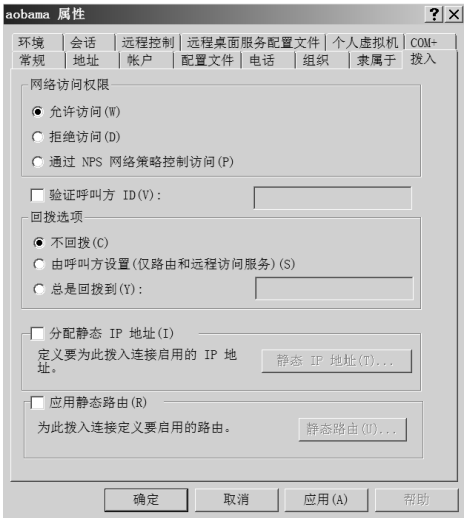


图 10-22　允许用户远程访问

如果远程访问是拨号连接方式，在“拨入”选项卡还可以设置回拨、分配静态 IP 地址和静态路由等。

- “不回拨”选项：指当用户拨号进来后，只要账户正确就可以与网络连接。
- “由呼叫方设置（仅路由和远程访问服务）”选项：指当远程访问服务客户机拨入远程访问服务器后，输入正确的账户，服务器会要求用户输入回拨的电话号码，然后挂断，由服务器对用户进行拨号，为远程用户节省电话费用。

- “总是回拨到”选项：指服务器对该用户的回拨号码做了事先规定，即使用户的账户被盗用，只要他使用的电话号码与服务器设置的不同，依然无法访问，该设置提高了远程访问的安全性。

注意：

在非域环境中，如果要使用户利用 VPN 服务器的本地用户账户来连接，可在 VPN 服务器上选择“本地用户和组”中的用户，设置本地用户的拨入属性。

10.2.4 配置客户机网络连接

配置好远程访问服务器后，还需要在客户机上建立 VPN 连接，才能进行远程访问，操作步骤如下所述。

STEP1 为远程用户设置 VPN 连接（以 Windows XP 为例）。VPN 客户端的 IP 地址为 200.100.1.2，打开网络连接，选择左侧的“创建一个新的连接”，打开“新建连接向导”页面，单击“下一步”按钮，如图 10-23 所示。

STEP2 在“网络连接类型”页面选择“连接到我的工作场所的网络”，单击“下一步”按钮，如图 10-24 所示。

图 10-23 新建连接向导

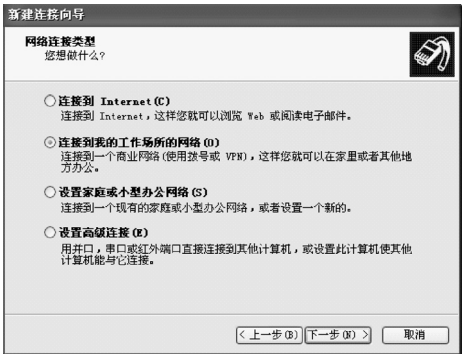


图 10-24 选择网络连接类型

STEP3 在“网络连接”页面选择“虚拟专用网络连接”，单击“下一步”按钮，如图 10-25 所示。

图 10-25 使用虚拟专用网络连接

STEP4 按照提示依次输入连接名和服务器地址（200.100.1.1），完成新建连接，如图 10-26 所示。

STEP5 在弹出的远程连接登录框中输入有远程访问权限的用户名和密码，单击“连接”，如图 10-27 所示。

图 10-26　完成新建连接

图 10-27　远程连接

STEP6 连接成功后，显示虚拟专用网络连接已经连接成功的页面，如图 10-28 所示。右键单击虚拟专用网络连接，选择“状态”，在网络连接状态对话框中选择“详细信息”选项卡，可以看到该客户端通过 VPN 方式连接到远程访问服务器的详细信息，如图 10-29 所示。此时远程用户犹如处在局域网内部一样，可以访问局域网内部的资源。

图 10-28　虚拟专用网络连接成功

图 10-29　连接的详细信息

10.3　任务 2：使用网络策略控制访问

通过搭建路由和远程访问服务可以让远程用户访问局域网内部，如果需要限制用户的登录时间和指定数据传输的加密方式，就需要配置网络策略服务（NPS）。

网络策略具有许多功能，如下所述。

- 限制允许用户连接的时间。
- 限制只有属于某个组的用户才可以连接远程访问服务器。
- 限制用户必须通过请求的方式连接。
- 限制用户必须使用请求的验证协议。
- 限制用户必须使用请求的数据加密方法。

ABC 公司要求能远程访问的用户必须属于 tech 组，而且只能在星期一到星期五 6:00 到 18:00 连接，必须采用 MS-CHAP-v2 验证方法。

10.3.1 新建网络策略

STEP1 在“路由和远程访问”窗口中右键单击“远程访问日志和策略”，选择“启动 NPS”，如图 10-30 所示。

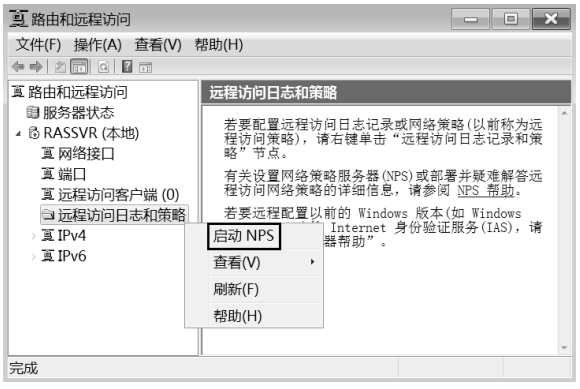


图 10-30 启动 NPS

STEP2 在打开的“网络策略服务器”（NPS）窗口中单击左侧窗格的“网络策略”，可以查看与设置网络策略，如图 10-31 所示。

图 10-31 “网络策略服务器”窗口

注意：

图 10-31 中已经有两个内置的网络策略，排列在上面的策略优先级高。当用户连接到远程访问服务器时，远程访问服务器会将此连接请求转交给网络策略服务器来检查，而网络策略服务器会先从上面的策略开始比对用户是否符合该策略所定义的条件。若符合，则执行此策略；若不符合，则依次比对第二个策略、第三个策略……只要有一个策略符合，之后的策略就不会再比对了。若没有任合一个策略符合，用户将无法连接到远程服务器。

STEP3 右键单击图 10-31 左侧窗格的“网络策略”，选择“新建”，如图 10-32 所示。

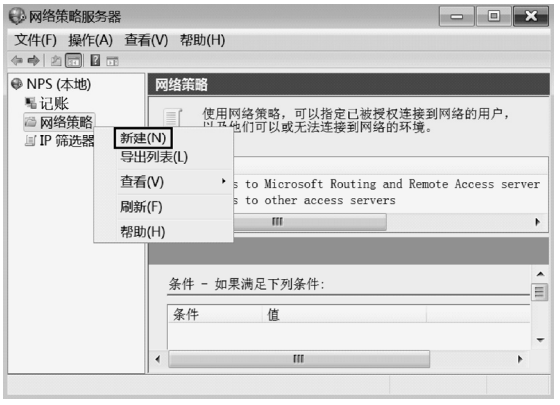


图 10-32　新建网络策略

STEP4 在“指定网络策略名称和连接类型”页面中为策略设置一个名称，然后在“网络访问服务器的类型”中选择“Remote Access Server(VPN-Dial up)”，表示此策略适用于由 VPN 服务器所传来的连接请求。如果要让此策略适用于所有类型的服务器，则选择“未指定”，单击“下一步”按钮，如图 10-33 所示。

图 10-33　指定网络策略名称和连接类型

STEP5 在“指定条件”页面中单击“添加”按钮，出现“选择条件”页面，选择“用户组”，单击“添加”按钮，如图 10-34 所示。

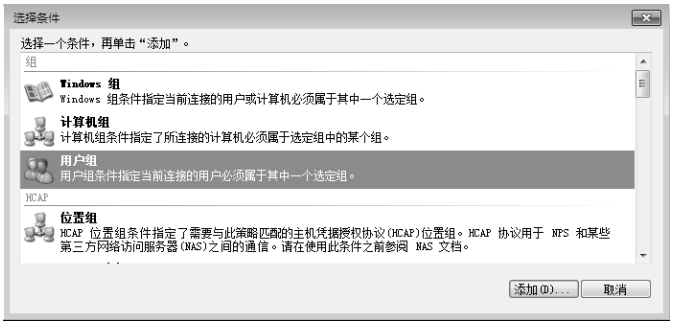


图 10-34　选择条件

STEP6 在“用户组”页面单击“添加组”按钮，添加 tech 组，单击“确定”按钮完成添加，如图 10-35 所示。

图 10-35　添加 tech 组

STEP7 单击“确定”按钮后返回到“指定条件”页面，在此页面中单击“添加”按钮，选择“NAS 端口类型”，再单击“添加”按钮，如图 10-36 所示。

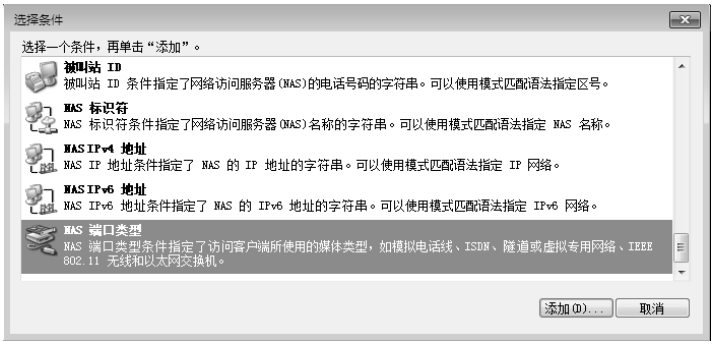


图 10-36　选择条件

STEP8 在“NAS 端口类型”页面中选择“Virtual（VPN）”，单击“确定”按钮，表示只有利用 VPN 来连接的用户才适用此策略，如图 10-37 所示。

STEP9 返回“指定条件”页面，单击“下一步”按钮，在出现的“指定访问权限”页面中选择“已授予访问权限”，单击“下一步”按钮，如图 10-38 所示。

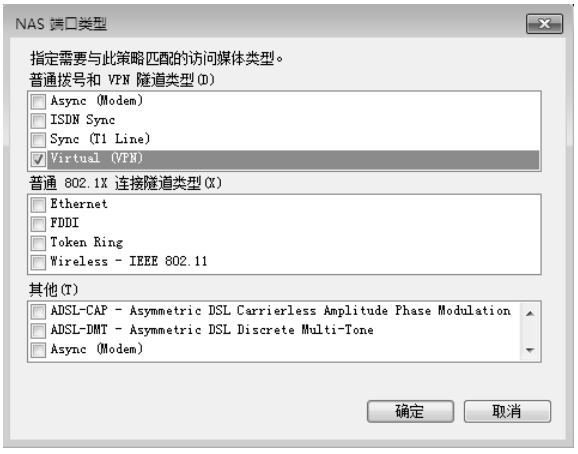


图 10-37　选择 NAS 端口类型

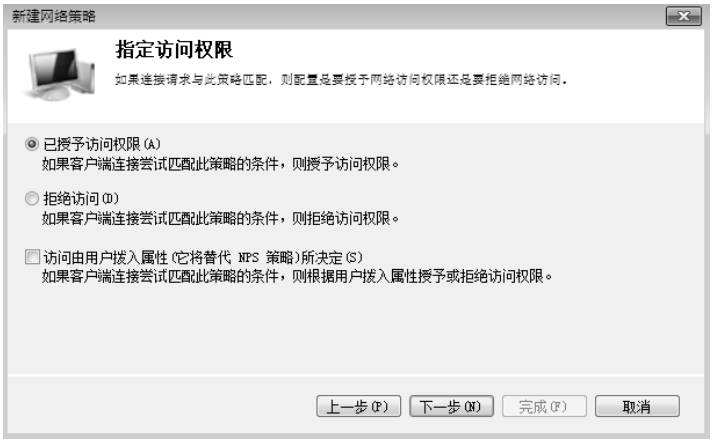


图 10-38　指定访问权限

STEP10 在“配置身份验证方法”页面确认已经选择 MS-CHAP-v2 后单击“下一步”按钮，如图 10-39 所示。

图 10-39　配置身份验证方法

STEP11 在“配置约束”页面中选择“日期和时间限制”，勾选“仅允许在这些日期和时间访问”，如图 10-40 所示。

图 10-40　配置时间和日期约束

STEP12 在图 10-40 中单击“编辑”按钮，选择允许和拒绝访问的时段，如图 10-41 所示。

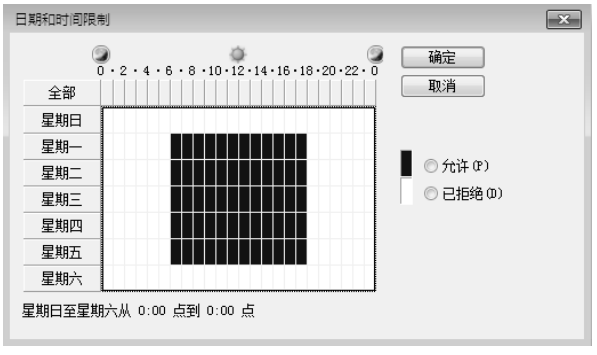


图 10-41　日期和时间限制

STEP13 返回“配置约束”页面，单击“下一步”按钮，在“配置设置”页面选择“加密”，如图 10-42 所示，确认已选择所有的加密方法，单击“下一步”按钮。

图 10-42　配置设置

STEP14 在“正在完成新建网络策略”页面中单击“完成”按钮，显示策略列表，如图 10-43 所示。新建策略位于策略列表的最上方，说明拥有最高的优先级。

图 10-43　显示策略列表

10.3.2　远程用户访问权限

远程用户是否允许连接远程访问服务器，要由用户账户的属性设置与网络策略的设置来决定。

右键单击新建的策略，选择“属性”，在策略属性页面的“概述”选项卡中可以配置访问权限，如图 10-44 所示。

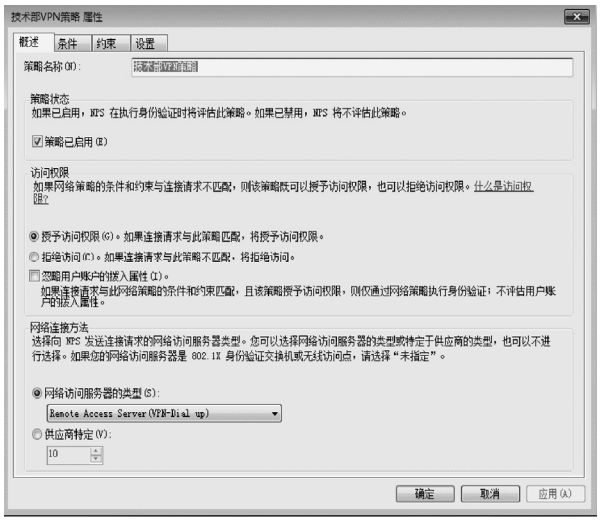


图 10-44　访问权限

使用访问权限，可以在连接请求匹配网络策略的条件和约束时，将策略配置为授予用户访问权限或拒绝用户访问。

- 授予权限：如果连接请求匹配策略中配置的条件和约束，则授予访问权限。
- 拒绝访问：如果连接请求不匹配策略中配置的条件和约束，则拒绝访问。

也可以使用每个用户账户的拨入属性授予访问权限或拒绝访问，在用户账户的拨入属性

上配置的“网络访问权限”将覆盖网络策略访问权限的设置。若将用户账户上的网络访问权限设置为“通过 NPS 网络策略控制访问”，则网络策略访问权限的设置将确定授予用户访问权限或拒绝用户访问。

可以将网络策略配置为“忽略用户账户的拨入属性”，当网络策略服务执行连接请求的授权时，它会检查用户账户的拨入属性，其中网络访问权限的设置值会影响是否授权用户连接到网络。

10.4 实训

实训环境

HT 公司员工出差期间需要访问公司局域网中文件服务器上的共享文件夹 files，文件服务器的 IP 地址为 172.16.1.2，实训示意图如图 10-45 所示。出差的员工使用 VPN 连接到公司局域网，VPN 服务器连接 Internet 的 IP 地址为 61.167.1.1。出差员工的计算机操作系统为 Windows XP，出差员工能使用 UNC 路径“\\172.16.1.2\files”访问局域网中的文件服务器。出于安全方面的考虑，需要限制员工只有在周一到周五的早 8:00 到晚 17:00 才能进行远程访问。

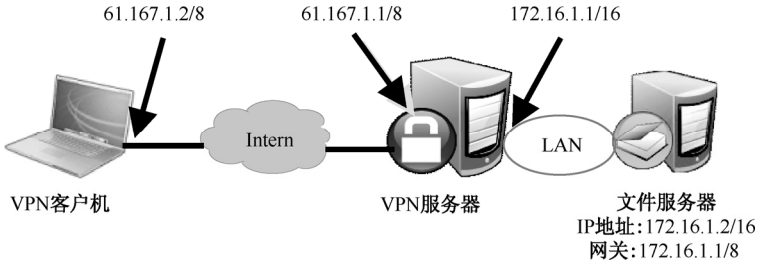


图 10-45 实训示意图

需求描述

- 在一台双网卡的服务器上启用路由和远程访问服务，此计算机作为 VPN 服务器。
- 在“Active Directory 用户和计算机”中设置用户的拨入权限。
- 配置远程访问策略。
- 建立并配置网络策略，限制访问时间。
- 用 VPN 客户端访问局域网。

10.5 习题

- VPN 的中文意思是什么？组成要素有哪些？
- 配置远程访问服务器需要哪些步骤？
- 远程访问服务必须是域环境吗？
- 如何配置远程访问客户端？
- 多个网络策略是如何匹配的？

第 11 章

PKI 与证书服务

项目需求：

ABC 公司随着业务的发展，要将域名为 www.abc.com 的 Web 站点升级为网上交易平台，开展网上订单、网络支付等业务，用户在访问时需要使用加密的信息传输协议，以保证用户密码和访问数据在传输时的安全性。

技能目标：

- 理解 PKI 相关知识
- 理解证书发放过程
- 掌握证书服务的安装方法
- 掌握企业 CA 的管理方法
- 掌握在 Web 服务器上设置 SSL 的方法

MEMO

11.1 知识介绍——PKI 概述

当在网络上传输数据时，这些数据可能会在发送过程中被拦截、篡改或执行各种不同类型的攻击行为，公钥基础结构（Public Key Infrastructure，PKI）可以确保数据发送的安全。

PKI 是通过使用公钥技术和数字证书来确保信息安全，并负责验证数字证书持有者身份的一种技术。PKI 让个人或企业能够安全地从事商业活动，企业员工可以在互联网上安全地发送电子邮件而不必担心信息被非法拦截。

在 PKI 中，各参与者都信任一个 CA（证书颁发机构），由该 CA 来核对和验证各参与者的身份。PKI 由公钥加密技术、数字证书、CA 和 RA（注册机构）等组成。数字证书用于用户的身份验证；CA 是 PKI 的核心，负责管理 PKI 中所有用户的数字证书的生成、分发、验证、撤销；RA 接受用户的请求，负责将用户的有关申请信息存档备案，存储在数据库中等待审核，并将审核通过的证书请求发送给 CA。

11.1.1 公钥加密技术

数据被加密后，必须经过解密才能读到数据内容。PKI 使用公钥加密技术将数据加密和解密。公钥加密技术需要两种密钥——公钥和私钥。公钥和私钥之间有如下关系。

- 公钥和私钥是成对生成的，这两个密钥互不相同，可以互相加密和解密。
- 不能根据一个密钥推算出另一个密钥。
- 公钥对外公开，私钥只有私钥持有人才知道。
- 私钥应该由私钥的持有人妥善保管。

公钥和私钥要配对使用，如果用公钥对数据进行加密，只有用相对应的私钥才能解密；如果用私钥对数据进行加密，那么只有用对应的公钥才能解密。根据两种密钥的使用顺序，可以分为数据加密和数字签名。

1．数据加密

数据加密确保只有预期的接收者才能够解密和查看原始数据，以提高机密性。在传送数据时，发送方使用接收方的公钥加密数据并传送；当接收方收到数据后，再用自己的私钥解密这些数据，数据加密的过程如图 11.1 所示。

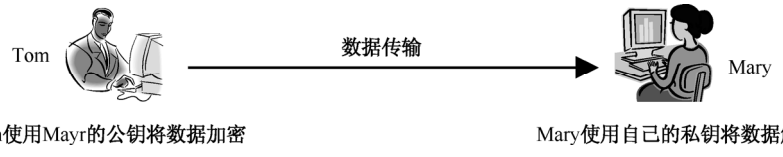


图 11-1 数据加密的过程

数据加密能确保发送数据的机密性，但不能检查数据在传输过程中是否完整，以及验证发送方的身份，要解决这个问题，还需要数字签名。

2．数字签名

数字签名具有以下功能。

- 身份验证：接收方可确认该发送方的身份标识。
- 数据完整性：证实消息在传输过程中内容没有被修改。
- 操作的不可否认性：其他用户不可能冒充发送方来发送消息。

用户可以通过数字签名确保数据的完整性和有效性，只需采用私钥对数据进行加密处理，由于私钥仅为个人拥有，从而能够证实签名消息的唯一性，数字签名的过程如图 11-2 所示。

图 11-2　数字签名的过程

如果第三方没有获得发送方的私钥，则无法冒充发送方进行数据签名，从而提供了一个安全确认发送方身份的方法。

11.1.2　PKI 协议

PKI 提供了完整的加密和解密解决方案，许多用于安全通信的协议和服务都是基于 PKI 来实现的。

1．SSL（Secure Socket Layer）安全套接字层

SSL 是一个以 PKI 为基础的安全协议，可确保数据在网络传输过程中不会被截取及窃听，并保证数据完整性，目前的浏览器都支持 SSL。SSL 协议位于 TCP/IP 协议与各种应用层协议之间，可分为以下两层。

- SSL 记录协议：建立在可靠的传输协议之上，为高层协议提供数据封装、压缩、加密等基本功能支持。
- SSL 握手协议：建立在 SSL 记录协议之上，用于在实际的数据传输开始前，对通信双方进行身份认证、协商加密算法、交换加密密钥等。

SSL 协议主要提供如下服务。

- 认证用户和服务器，确保数据发送到正确的客户机和服务器上。
- 加密数据以防止数据中途被窃取。
- 维护数据的完整性，确保数据在传输过程中不被改变。

SSL 协议的工作流程分为两个阶段：服务器认证阶段和用户认证阶段。

（1）服务器认证阶段

① 客户端向服务器发送一个开始信息，以便开始一个新的会话连接。

② 服务器根据客户的信息确定是否需要生成新的通信密钥，如果需要则服务器在响应客户的“Hello”信息时，将包含生成通信密钥所需的信息也发送给客户端。

③ 客户根据收到的服务器响应信息，产生一个通信密钥，并用服务器的公开密钥加密后传给服务器。

④ 服务器解密后获得通信密钥，并返回给客户一个通信密钥加密信息，客户以此信息认证服务器。

（2）用户认证阶段

完成服务器认证后，服务器会发送一个信息给客户，客户则返回数字签名后的信息和其公开的密钥，从而向服务器提供认证。

2．HTTPS（Hypertext Transfer Protocol Secure）安全超文本传输协议

HTTPS 用于对数据进行加密和解密，并返回网络上传回的结果。HTTS 应用安全套接字层（SSL）作为 HTTP 应用层的子层，通过该子层实现身份验证与加密通信，被广泛应用于互联网上安全敏感的通信，如网上支付。HTTPS 使用端口 443，而不是使用 TCP/IP 端口 80 通信。

3．IPSec（IP Security）

IPSec 协议是应用广泛、开放的 VPN 安全协议，目前已经成为最流行的 VPN 解决方案，包括 AH 和 ESP。

AH（Authentication Header，验证头）协议为 IP 通信提供数据源认证和数据完整性保护等功能。ESP（Encapsulating Security Payload，安全负载封装）提供数据保密、数据源身份认证、数据完整性保护、重放攻击保护等功能。

11.2 知识介绍——证书颁发机构

证书颁发机构 CA（Certificate Authority，证书颁发机构）也称为数字证书认证中心，是 PKI 应用中权威的、可信的、公证的第三方机构，也是电子交易中心信赖的基础。CA 的主要功能是负责产生、分配并管理所有参与网上交易的实体所需的身份认证数字证书。

11.2.1 证书

为保证网络上信息传输的安全，除了在通信传输中采用加密算法措施，还必须建立一种信任验证机制，通信各方必须有一个可以被验证的标识，即数字证书。

PKI 中的数字证书简称证书，它把公钥和拥有对应私钥的主体标识信息捆绑在一起，证书的主体可以是用户、计算机和服务等。证书可以用于 Web 服务器和用户身份验证以及保证电子邮件安全等。

数字证书是一种权威性的电子文档，是由权威、公正的第三方机构 CA 中心签发的，以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字和签名验证，确保网上信息传输的机密性和完整性。使用了数字证书，即使发送的信息在网上被截获，甚至丢失了个人账户、密码等信息，仍可以保证账户和资金的安全。

数字证书中包含使用者公钥、使用者标识信息（名称和电子邮件等）、证书有效期限、

颁发者标识信息、颁发者数字签名等数据信息。

11.2.2　CA 的作用

CA 可以自己创建，也可以由第三方机构搭建。在复杂的认证体系中，CA 分不同的层次，各层 CA 按照目录结构形成一棵树。在 CA 体系结构中，根 CA 处于核心地位，功能是认证授权，具体如下所述。

- 处理证书申请。
- 鉴定申请者是否有资格接收证书。
- 向申请者颁发或拒绝颁发证书。
- 接收并处理最终用户的数字证书更新请求。
- 接收最终用户数字证书的查询和撤销。
- 产生和发布证书吊销列表。
- 数字证书、密钥和历史数据归档。

11.2.3　CA 的类型

CA 有企业 CA 和独立 CA 两大类。企业 CA 又分为企业根 CA 和企业子级 CA；独立 CA 也分为独立根 CA 和独立子级 CA。

1．企业根 CA

企业根 CA 需要 Active Directory 域，可以将企业根 CA 安装到域控制器或成员服务器中。企业根 CA 发放证书的对象是域用户，非域用户无法向企业根 CA 申请证书。当域用户申请证书时，企业根 CA 可以从 Active Directory 得知该用户的相关信息，并据此决定该用户是否有权申请所需证书。

2．企业子级 CA

企业子 CA 也需要 Active Directory 域，企业子 CA 适合用来发放保护电子邮件安全和 SSL 网站安全连接等证书。企业子 CA 必须向其父 CA（如企业根 CA）取得证书之后，才能正常运行，企业子 CA 也可以发放证书给下一层子级 CA。

3．独立根 CA

独立根 CA 的角色与功能类似于企业根 CA，但不需要 Active Directory 域。扮演独立根 CA 角色的计算机可以是独立服务器、成员服务器或域控制器。无论是否为域用户，都可以向独立根 CA 申请证书。

4．独立子级 CA

独立子级 CA 的角色与功能类似于企业子级 CA，但不需要 Active Directory 域。扮演独立子级 CA 角色的计算机可以是独立服务器、成员服务器或域控制器。无论是否为域用户，都可以向独立子级 CA 申请证书。

11.2.4 证书颁发过程

假设某个用户要申请一个证书，以实现安全通信，证书的申请与发放过程如图 11-3 所示。

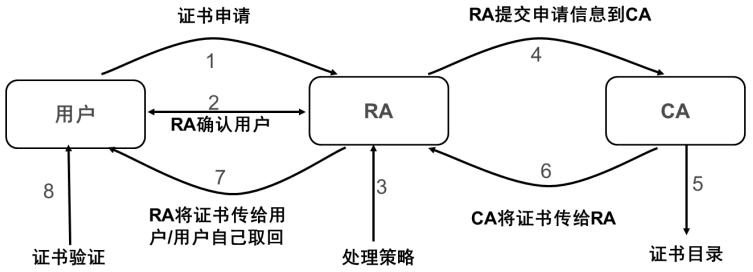


图 11-3 证书的申请与发放过程

① 证书申请。用户生成密钥对，根据个人信息填好申请证书的信息并提交证书申请信息。

② RA 确认用户。在企业内部网通常使用手工验证方式，这样更能保证用户信息的安全性和真实性。

③ 处理证书策略。如果验证请求成功，系统指定的策略就被运用到这个请求上，如名称、密钥长度的约束等。

④ RA 提交用户申请信息到 CA。RA 用自己的私钥对用户申请信息进行签名，保证用户申请信息是 RA 提交给 CA 的。

⑤ CA 用自己的私钥对用户的公钥和用户信息的 ID 进行签名，生成电子证书。这样，CA 就将用户的信息和公钥捆绑在一起了。然后，CA 将用户的数字证书和用户的公用密钥公布到目录中。

⑥ CA 将电子证书传送给批准该用户的 RA。

⑦ RA 将电子证书传送给用户或者用户自动取回。

⑧ 用户验证 CA 颁发的证书，确保自己的信息在签名过程中没有被篡改，而且通过 CA 的公钥验证这个证书确实由所信任的 CA 机构颁发。

11.3 任务 1：安装证书服务

在 Windows Server 2008 R2 操作系统中，证书服务不是默认安装的服务，需要手工添加，以下步骤以域环境下安装企业根 CA 为例。

STEP1 用域系统管理员身份登录，打开“开始”→“管理工具”→“服务器管理器”窗口，单击“角色”页面的“添加角色”，打开“添加角色向导”页面。

STEP2 单击“下一步”按钮，进入“选择服务器角色”页面，选择“Active Directory 证书服务”，单击“下一步”按钮，如图 11-4 所示。

STEP3 在“Active Directory 证书服务”页面单击“下一步”按钮，在“选择角色服务”页面中选择“证书颁发机构”和“证书颁发机构 Web 注册”，在弹出的提示框中单击“添加所需的角色服务”来安装所需的角色服务和功能，如图 11-5 所示。

STEP4 返回到“选择角色服务”页面，单击“下一步”按钮，如图 11-6 所示。

图 11-4　选择服务器角色

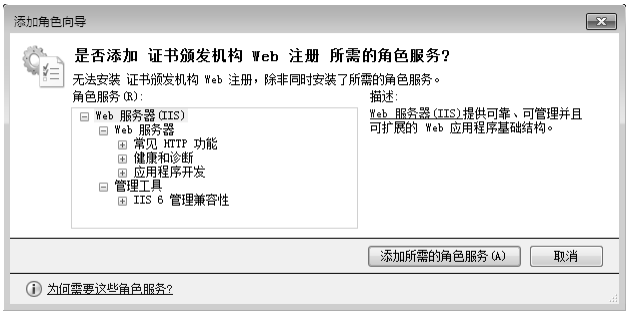


图 11-5　添加所需的角色服务

图 11-6　选择角色服务

STEP5 在“指定安装类型”页面选择“企业”，单击“下一步”按钮，如图 11-7 所示。

注意:

只有在域环境中安装证书服务时才可以选择企业 CA，如果安装证书服务的计算机在工作组环境下，将无法选择企业 CA，只能安装独立 CA。

图 11-7　指定安装类型

STEP6 在“指定 CA 类型”页面选择“根 CA”，单击“下一步”按钮，如图 11-8 所示。

图 11-8　指定 CA 类型

STEP7 在“设置私钥”页面选择“新建私钥”，单击“下一步”按钮，如图 11-9 所示。

STEP8 在“为 CA 配置加密”页面，使用默认的加密服务提供程序、哈希算法和密钥长度，单击“下一步”按钮，如图 11-10 所示。

- 加密服务提供程序（CSP）：是执行身份验证、编码和加密服务的程序。基于 Windows 的应用程序通过 Microsoft 加密应用程序编程接口访问该程序。CSP 列表中有计算机上满足以下配置选项组和所指定条件的所有可用程序。
- 哈希算法：通过此选项可以选择高级哈希算法。默认情况下，可以使用以下算法：AES-GMAC、MD2、MD4、MD5、SHA1、SHA256、SHA384、SHA512。
- 密钥长度：通过此选项，可以指定在所选算法中使用密钥所需的最小长度。默认情况下将使用计算机上所选算法支持的最小密钥长度。密钥长度越长越安全，根 CA 应使用长度至少 2048 位的密钥。

图 11-9　设置私钥

图 11-10　为 CA 配置加密

注意:
如果是在已经安装过 CA 的计算机上安装，则可以选择“使用现有私钥”。

STEP9　在“配置 CA 名称”页面设置 CA 名称，这里采用默认名称，如图 11-11 所示。

STEP10　在“设置有效期”页面使用默认的 5 年有效期，单击“下一步”按钮；在“配置证书数据库”页面使用默认的保存位置，单击“下一步”按钮。

STEP11　在“Web 服务器（IIS）”页面单击“下一步”按钮；在“选择角色服务”页面单击“下一步”按钮；最后，在“确认安装选择”页面单击“安装”按钮；在“安装结果”页面显示安装成功，单击“关闭”按钮。

STEP12　安装完成后，可以选择“开始”→“管理工具”→“证书颁发机构”，通过打开证书颁发机构管理器来管理证书的颁发，如图 11-12 所示。

图 11-11　配置 CA 名称

图 11-12　证书颁发机构管理器

STEP13 用户可以使用 Web 浏览器访问“http://CA 主机名或 IP 地址/certsrv/”（访问该目录时需要提供用户名和密码）来连接 CA 网站，申请证书，如图 11-13 所示。

图 11-13　使用 Web 浏览器申请证书

11.4　任务 2：SSL 网站证书应用

在访问 Web 网站时，如果没有安全措施，用户访问的数据有可能被他人使用网络工具捕获并分析出来，为网站申请 SSL 证书，连接网站才安全。如果网站要对一般 Internet 用户提供服务，应该向权威的 CA 申请证书，如 VerSign 和 Entrust 等；如果网站只是对内部员工和企业合作伙伴提供服务，则可以利用 Active Directory 证书服务来搭建 CA，并向 CA 申请证书。

11.4.1　申请与颁发证书

为 Web 网站应用证书前必须先生成证书申请，用以标识证书将用于哪个 Web 站点，下面以为 www.abc.com 网站申请证书为例说明如何申请并应用证书。

STEP1　在 Web 服务器上打开“管理工具”中的“Internet 信息服务（IIS）管理器”，在左侧窗格选择服务器名称，双击中间窗格的“服务器证书”，如图 11-14 所示。

图 11-14　服务器证书

STEP2　单击右侧窗格的“创建证书申请”，如图 11-15 所示。

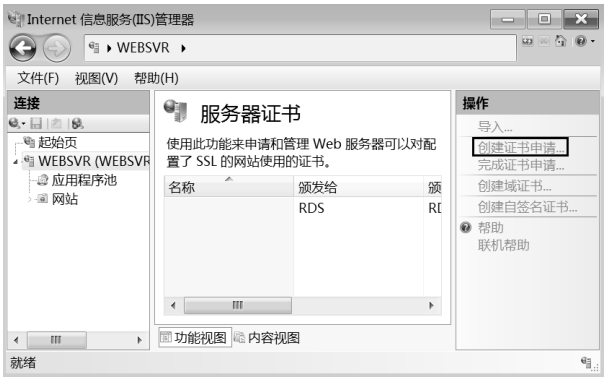


图 11-15　创建证书申请

STEP3　打开“可分辨名称属性”页面，输入证书相关信息，单击“下一步”按钮，如图 11-16 所示。

图 11-16　输入证书信息

STEP4 在“加密服务提供程序属性”页面，使用默认的加密程序和密钥长度，单击“下一步”按钮，如图 11-17 所示。图中的“位长”用来指定网站公钥的长度，位长越长，安全性越高，但性能越低，一般选择默认的 1024 位即可。

图 11-17　加密服务提供程序属性

STEP5 在“文件名”页面为该证书申请指定一个文件名和保存位置，单击“完成”按钮，完成证书申请的创建，如图 11-18 所示。打开证书申请文件 C:\certificate.txt，可见证书申请文件是 Base64 编码。

图 11-18　指定证书申请的文件名

STEP6 通过浏览器访问证书服务器的虚拟目录“http://192.168.1.1/certsrv/”，单击“申请证书”，如图 11-19 所示。

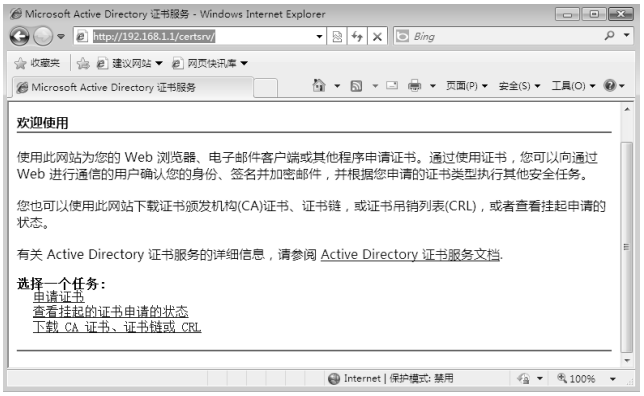


图 11-19　申请证书

STEP7 在“申请一个证书”页面单击“高级证书申请”，如图 11-20 所示。

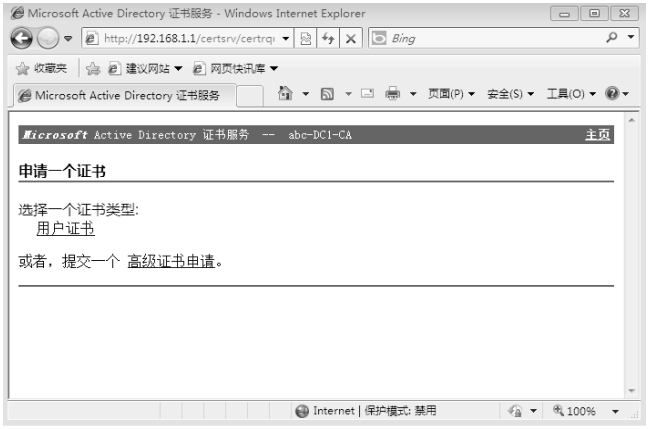


图 11-20　高级证书申请

STEP8 在“高级证书申请”页面中，选择第二项，使用 base64 编码的证书申请，如图 11-21 所示。

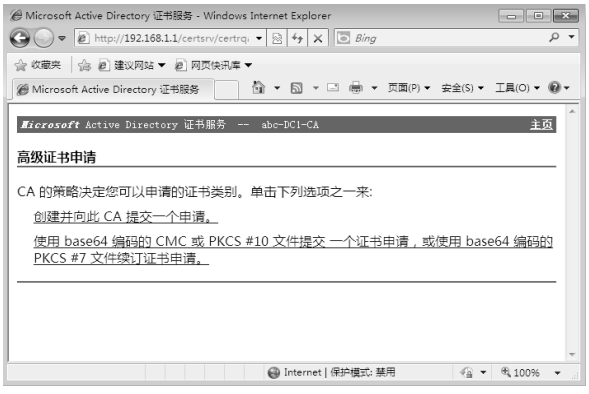


图 11-21　使用 base64 编码的证书申请

STEP9 打开 STEP5 中保存的证书申请文件 c:\certificate.txt，复制全部文件内容。在“提交一个证书申请或续订申请”页面，将复制的证书申请内容粘贴到“保存的申请：”文本框中，在“证书模板”下拉列表中选择“Web 服务器”，单击“提交”按钮，如图 11-22 所示。

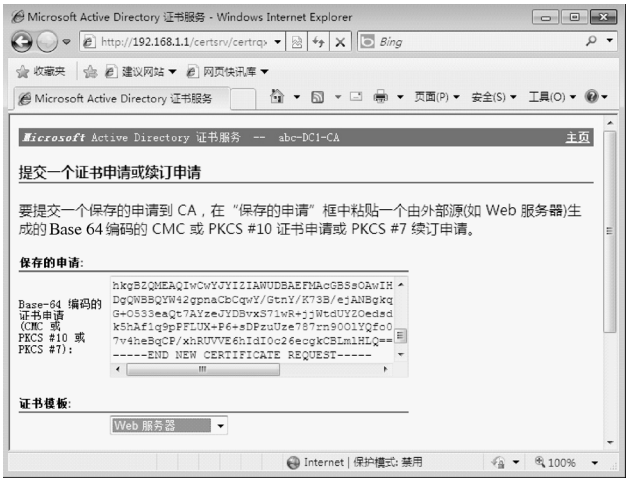


图 11-22 提交证书申请

注意：

如果使用的是企业 CA，在提交申请后 CA 会自动颁发证书，以上操作是使用企业 CA，所以证书会自动颁发；如果是独立 CA，则需要人工操作颁发证书，打开独立 CA，在左侧窗格选择“挂起的申请”，在右侧窗格右键单击申请，选择“所有任务”→“颁发”，为该申请颁发证书。

STEP10 在“证书已颁发”页面，选择“Base 64 编码”，单击“下载证书”，将证书保存到本地，如图 11-23 和图 11-24 所示。

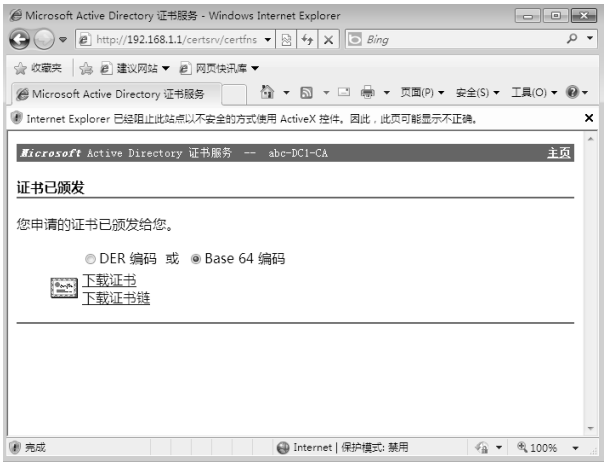


图 11-23 证书已颁发

图 11-24 保存证书

11.4.2　安装与使用证书

将证书下载到本地后，就可以为指定的 Web 站点应用该证书。

STEP1 单击图 11-15 中右侧窗格的“完成证书申请”，在“指定证书颁发机构响应”页面，输入已下载的数字证书文件的路径和文件名，并给该文件定义一个好记名称，如图 11-25 所示指定 CA 响应文件，单击“确定”按钮，完成证书的申请。

图 11-25　指定 CA 响应文件

STEP2 展开“Internet 信息服务（IIS）管理器”左侧窗格的节点，选择需要使用该证书的站点，单击右侧窗格的“绑定”，如图 11-26 所示设置站点绑定。

STEP3 在“网站绑定”页面单击“添加”，出现“添加网站绑定”对话框，在“类型”下拉列表框中选择“https”，在“SSL 证书”下拉列表框中选择先前安装的证书“web”，单击“确定”按钮，如图 11-27 所示。

STEP4 在客户机中用户使用 HTTPS 协议连接网站。如果客户机没有信任发放 SSL 证书的 CA，会出现警告界面。单击“是”按钮，继续浏览此网站，如图 11-28 所示使用 SSL。

图 11-26　设置站点绑定

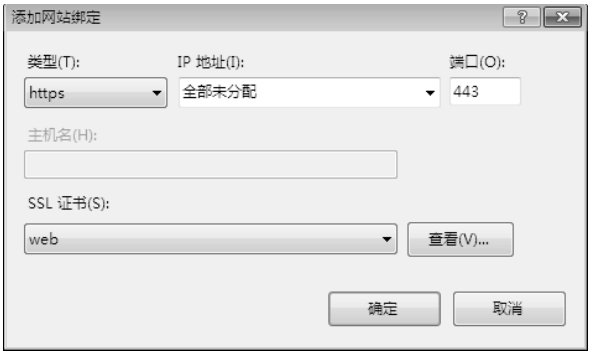


图 11-27　添加网站绑定

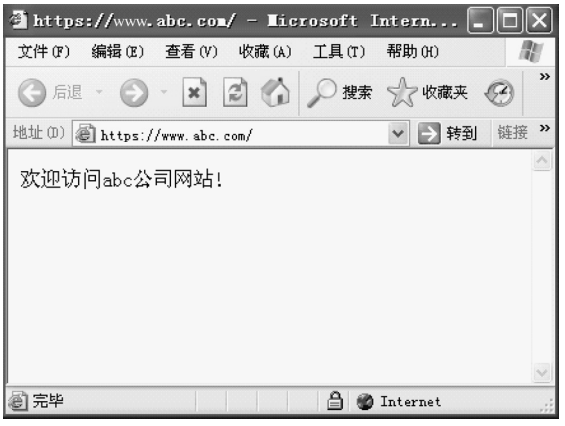


图 11-28　使用 SSL

注意：

网站服务器与浏览网站的客户机都应该信任发放 SSL 证书的 CA，否则客户端浏览器在使用“HTTPS”连接网站时会显示警告信息。如果是企业 CA，而且网站服务器与浏览网站的客户机都是域成员，则会自动信任企业 CA，否则要手动执行信任 CA 的操作。

通过修改站点的 SSL 设置，可以配置是否强制用户使用 SSL 方式连接站点。展开“Internet 信息服务（IIS）管理器”左侧窗格的节点，选择需要使用证书的站点，双击中间窗格的“SSL 设置”，进入 SSL 页面，如图 11-29 所示。如果需要强制用户使用 SSL 方式连接站点，则选择“要求 SSL”。选择此项后，用户只能以 HTTPS 协议连接站点。

在“SSL 设置”页面还可以设置是否需要客户端证书。

- 忽略：无论用户是否拥有证书，都将被授予访问权限，客户端不需要申请和安装客户端证书。
- 接受：用户可以使用客户端证书访问资源，但证书并不是必须的，客户端不需要申请和安装客户端证书。
- 必需：服务器在将用户与资源连接之前要验证客户端证书，客户端必须申请和安装客户端证书。

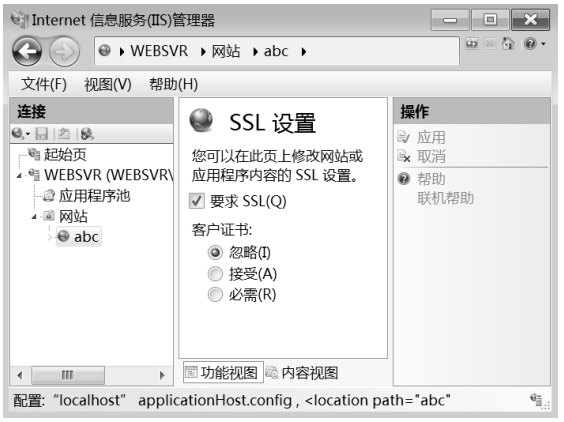


图 11-29　SSL 设置

11.4.3　导入与导出证书

如果安装了证书的网站需要重新创建，新网站不需要重新申请和安装证书，只需在网站正常时将安装的证书导出为一个文件，存放在可靠的地方，重新搭建网站后再导入证书即可。

1. 导出证书

STEP1　在 Web 服务器上打开“Internet 信息服务（IIS）管理器”，选择服务器名称，双击中间窗格的“服务器证书”，打开如图 11-30 所示的页面，显示了当前服务器安装的证书。

图 11-30　服务器证书

STEP2　选择要导出的证书，单击右侧的“导出”按钮，在“导出证书”对话框中指定导出路径、文件名及密码，单击“确定”按钮，如图 11-31 所示。

图 11-31　导出证书

2. 导入证书

重建完 Web 服务器后就可以导入先前导出保存的证书，不要求还是同一台服务器，但要保证使用该证书的站点的域名或 IP 地址要与证书相匹配。

在重建的 Web 服务器上打开“Internet 信息服务（IIS）管理器”，选择服务器名称，双击中间窗格的“服务器证书”，单击右侧操作窗格的“导入”，在“导入证书”对话框中，输入证书路径、文件名和密码，单击“确定”按钮，完成证书导入，如图 11-32 所示。

图 11-32　导入证书

11.5　实训

实训环境

HT 公司的网站域名为 www.huatian.com，随着公司业务的发展，公司欲将该网站发展成为网上交易平台，因此在用户访问时，需要保证用户密码和访问的数据在传输时的安全性。环境设计如图 11-33 实训示意图所示。

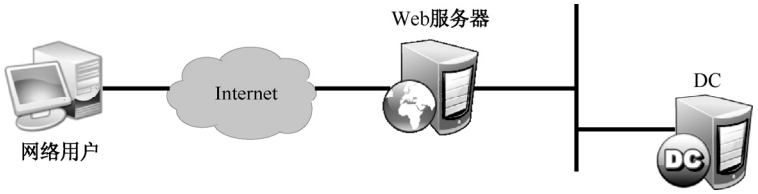


图 11-33　实训示意图

需求描述

- 安装 CA 证书服务。
- 在 Web 服务器上生成 Web 证书申请。
- 通过 IE 浏览器提交证书申请。
- 证书申请颁发后，下载 Web 服务器证书。
- 为 Web 服务器安装证书。
- 在 Web 服务器上配置 SSL。
- 使用 HTTPS 协议访问网站验证结果。

11.6　习题

- 什么是数据加密，简述其主要过程。
- 什么是数字签名，简述其主要过程。
- 证书中通常会包含哪些信息？
- CA 有哪些类型？
- 企业 CA 和独立 CA 有什么区别？

第 12 章

远程桌面服务（RDS）

项目需求：

ABC 公司有一些低配置的 PC 无法运行当前高版本的办公用软件，为了降低办公成本和管理员维护工作量，决定在运行 Windows Server 2008 R2 的服务器上部署远程桌面服务，为低配置的计算机提供应用程序访问，同时希望用户可以直接双击软件图标就能访问服务器上的程序，从而降低用户操作复杂度。

技能目标：

- 了解常用终端和远程桌面服务的作用
- 学会部署远程桌面服务
- 学会使用 RemoteApp 部署软件

MEMO

12.1 知识介绍——远程桌面服务概述

远程桌面服务（Remote Desktop Service，RDS）在 Windows Server 2008 R2 之前的版本中称为终端服务，可让用户（终端）访问在远程桌面服务器（主机）上安装的基于 Windows 的程序，还能访问完整的 Windows 桌面，主机与终端如图 12-1 所示。管理员可以在服务器上集中部署应用程序，以虚拟化的方式为用户提供访问，用户不必在自己的计算机上安装应用程序。当用户通过远程桌面调用服务器上的应用程序时，此程序如同运行在自己的计算机上，从而提高了工作效率，节约了维护成本。

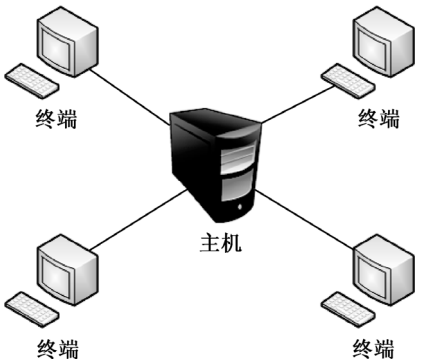


图 12-1 主机与终端

1. 终端

终端是与计算机主机相连的用户端设备，终端从键盘或鼠标接收用户的输入数据，并将这些输入数据发送到位于中心的计算机主机，由主机处理用户的请求并输出到终端显示器上。常用作终端的设备有以下几种。

（1）瘦客户机（Thin Client）

瘦客户机是基于 PC 工业标准设计的小型行业商用机，如图 12-2 所示。瘦客户机没有高速的 CPU 和大容量内存，使用低功耗的处理器和小型内存，没有硬盘，使用固化的小型操作系统，通过网络使用服务器的计算和存储资源，为企业降低了 IT 投入和维护成本。

（2）PC（Personal Computer）

在 PC 上安装并运行终端仿真程序，使 PC 可以连接并使用服务器的计算和存储资源。远程桌面连接如图 12-3 所示，在 Windows 7 终端上运行“远程桌面连接”程序连接 Windows 2008 R2 的主机。

图 12-2 瘦客户机

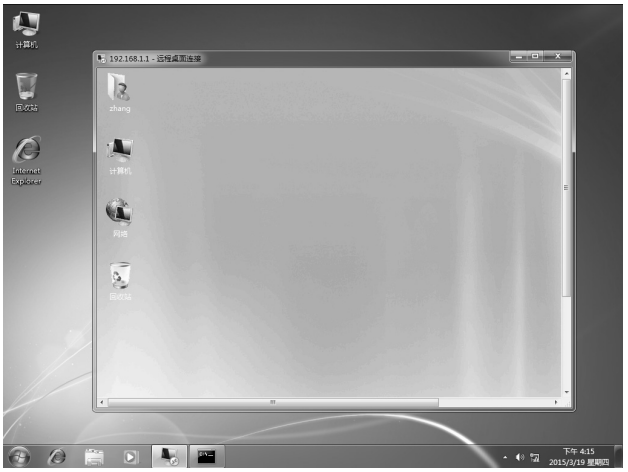


图 12-3 远程桌面连接

（3）手机终端

手机终端是手机无线网络接收端的简称，使用无线网络与主机相连，只要扫描相应的二维码或输入登录账号、密码等信息，就可以连接远程计算机，管理或控制计算机资源。

2．远程桌面服务

微软公司的远程桌面服务和思杰公司的桌面虚拟化（Citrix XenDesktop）都可以作为服务器，为瘦客户端和终端仿真程序提供服务。Windows Server 2008 R2 的远程桌面服务可以提供应用程序部署、远程桌面 Web 访问等多项功能，各服务功能如下所述。

- 远程桌面会话主机：用来承载基于 Windows 的程序或完整的 Windows 桌面，用户可连接到远程桌面会话主机服务器来运行程序、保存文件，以及使用该服务器上的网络资源。
- 远程桌面虚拟化主机：集成了 Hyper-V 以托管虚拟机，并将这些虚拟机作为虚拟桌面提供给用户。
- 远程桌面授权：管理终端到服务器连接所需的远程桌面服务客户端访问许可证，客户端要拥有访问许可证才可以连接到终端服务器。
- 远程桌面连接代理：通过网络负载平衡在一个“场”中部署多台远程桌面服务器，提供高可靠性。
- 远程桌面网关：允许用户从 Internet 连接到远程桌面服务器，远程桌面网关将会话封装在加密的 HTTPS 会话中，提供安全性。
- 远程桌面 Web 访问：允许用户通过 Web 浏览器访问 RemoteApp 和桌面连接。

12.2　任务 1：部署远程桌面服务

远程桌面服务是 Windows Server 2008 R2 的服务器角色，与其他服务器角色部署方法相同。

1．添加远程桌面服务

STEP1　在如图 12-4 所示的添加角色向导中选择“远程桌面服务”，单击“下一步”按钮，在出现的“远程桌面服务简介”页面中直接单击“下一步”按钮。

STEP2　在如图 12-5 所示的“选择角色服务”页面中选择需要的角色服务，这里选择“远程桌面会话主机”和“远程桌面 Web 访问”两个选项，支持此功能的角色也一并安装。

STEP3　在如图 12-6 所示的页面中选择是否使用网络级身份验证，这里选择“不需要网络级身份验证”，即兼容低版本的 Windows 客户端，单击“下一步”按钮。

STEP4　部署远程桌面服务需要购买微软的授权许可证，由于有 120 天的宽限期，可以在“指定授权模式”页面选择“以后配置”。单击“下一步”按钮，选择允许访问远程桌面会话主机服务器的用户或组，这些用户会被添加到 Remote Desktop Users 组中，如图 12-7 所示，默认只有 Administrator 组可以访问。

图 12-4　添加远程桌面服务

图 12-5　添加角色服务

图 12-6　指定远程桌面会话主机的身份验证方法

图 12-7　选择允许访问远程桌面会话主机服务器的用户或组

STEP5 按照安装提示，安装 IIS 的默认角色服务，单击“安装”按钮开始安装。安装完成后，显示安装结果，并提示需要重新启动服务器才能完成安装过程，如图 12-8 所示。重新启动后，显示安装成功。

图 12-8　安装结果

2．远程桌面会话主机配置

远程桌面服务安装后，用户就可以通过远程桌面连接到服务器了。依次打开服务器的“开始”→“管理工具”→“远程桌面”→“远程桌面会话主机配置”窗口，如图 12-9 所示。默认已经创建一个 RDP（Remote Desktop Protocol）连接，如果服务器安装有多个网卡，可以为每块网卡单独配置一个 RDP 连接。在此窗口中还可以配置或修改用户连接设置，如限制用户在服务器上只能进行一个会话，可以最大限度地减少在服务器上创建的远程会话数。

图 12-9　远程桌面会话主机配置

双击图 12-9 中的现有连接，出现如图 12-10 所示连接属性对话框，可以修改连接设置、连接安全性等。

图 12-10　连接属性

3．远程桌面服务管理

依次打开服务器的“开始”→“管理工具”→“远程桌面”→“远程桌面服务管理器”窗口，如图 12-11 所示，可查看服务器上的用户、会话、进程的有关信息并进行监视，还可以执行如强制注销用户、断开连接、给用户发送消息等管理任务。打开操作窗格中的“状态”选项，还可以查看有关连接的详细信息。

图 12-11　远程桌面服务管理器

4．连接远程桌面服务器

客户端要连接远程桌面服务器，首先要具有合法的用户，如果要添加 / 删除远程桌面用户，可以通过内置组“Remote Desktop Users”来进行。在客户端计算机上打开“程序”→“附件”→“远程桌面连接”窗口，输入服务器域名或 IP 地址，单击“连接”按钮，根据提示输入远程桌面用户名和密码，如图 12-12 所示，即可连接远程桌面服务器。

图 12-12　输入远程桌面用户名和密码

12.3　任务 2：部署 RemoteApp

RemoteApp 能使程序通过终端服务进行远程访问，就好像运行在用户的本地计算机上一样，这些程序称为 RemoteApp 程序。RemoteApp 程序与客户端的桌面集成在一起，而不是在远程桌面服务器中向用户显示。用户可以通过以下方式访问 RemoteApp 程序。

- 使用 Web 浏览器在网站上访问程序链接。
- 双击由管理员创建并分发的.rdp 文件。
- 双击由管理员使用 Windows Installer(.msi)程序包创建并分发的程序图标。

1．添加 RemoteApp 程序

STEP1 依次单击“开始”→“管理工具”→“远程桌面服务”→“RemoteApp 管理器”，打开如图 12-13 所示的窗口，在此窗口中可以添加 RemoteApp 程序，并对其进行管理，可以创建.rpd 或者.msi 程序包。

图 12-13　RemoteApp 管理器

STEP2 单击图 12-13 中的“添加 RemoteApp 程序”，打开“RemoteApp 向导”窗口，根据向导提示，选择要提供给终端用户的应用程序，如图 12-14 所示，单击“下一步”按钮，完成添加。

图 12-14　添加 RemoteApp 程序

2．访问 RemoteApp 程序

STEP1 用户可以在客户端使用浏览器访问并运行应用程序，实现远程桌面 Web 访问。打开客户机的浏览器，输入 http://服务器 IP 地址或主机名/rdweb，如图 12-15 所示，输入有权登录该站点的用户名和密码，单击“登录”按钮。

图 12-15　远程桌面 Web 访问（1）

STEP2 远程桌面 Web 访问需要运行 ActiveX 控件，页面顶端弹出提示信息，单击提示信息，在弹出的快捷菜单中选择“运行加载项”，单击“运行”按钮，在如图 12-16 所示网页中可以查看可用程序列表。

图 12-16　远程桌面 Web 访问（2）

STEP3 单击应用程序图标，弹出如图 12-17 所示的程序运行提示，单击“连接”按钮，输入具有远程访问权限的用户名和密码，即可运行应用程序，如图 12-18 所示运行 QQ。

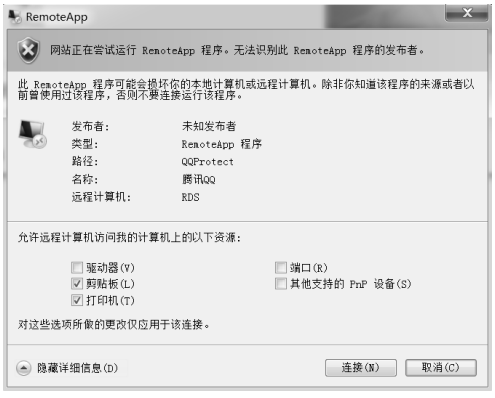


图 12-17　程序运行提示

图 12-18　运行 QQ

3．创建.rdp 文件

将 RemoteApp 程序打包成.rdp 文件，复制到用户的计算机上，用户运行这些程序更方便。在如图 12-13 所示的“RemoteApp 管理器”窗口，选择 RemoteApp 程序，单击“创建.rdp 文件”，出现如图 12-19 所示的 RemoteApp 向导。单击“下一步”按钮，指定.rdp 文件的保存路径、连接端口等选项，如图 12-20 所示。把创建完成的.rdp 文件复制到客户机，用户可双击运行，简化操作步骤。创建 Windows Installer 程序包和创建.rdp 文件方法相似，不再赘述。

图 12-19　RemoteApp 向导（1）

图 12-20　RemoteApp 向导（2）

12.4　实训

实训环境

HT 公司 8 年前购买的一批 PC 内存小、处理器版本低、硬盘空间小，公司为了节约成本，想继续使用这些计算机作为日常办公用机器。这些低配置的计算机作为终端，与远程服务器相连，将日常办公用软件安装在服务器上，终端用户可在自己的计算机上轻松使用服务器上的软件。

需求描述

- 在服务器上安装远程桌面服务。
- 在服务器上安装应用程序。
- 添加可访问远程桌面的用户。
- 添加 RemoteApp 程序。
- 创建.rdp 文件并复制到客户机。

12.5　习题

- 利用网络了解瘦客户机的品牌和应用范围。
- Windows Server 2008 R2 远程桌面服务与 Windows 7 远程桌面有什么区别？
- RemoteApp 可以创建哪格式的文件？
- 访问 RemoteApp 程序有哪些方法？

第 13 章

虚拟化服务

项目需求：

ABC 公司网络中心经过多年的建设已经部署了 DNS 服务器、文件服务器、DHCP 服务器、Web 服务器、远程访问服务器，近期公司又要部署数据库服务器、邮件服务器，由于旧服务器已经连续运行多年，系统性能下降，无法满足需求。公司购置了一台高性能计算机，要将所有服务整合到一台计算机上，由于各服务运行在不同的操作系统平台上，需要将新购置的高性能计算机虚拟成多台计算机，分别安装操作系统并提供服务，既能减少资金投入，又方便管理，提高计算机利用率。

技能目标：

- 理解虚拟化作用
- 会部署虚拟化服务
- 会安装和管理虚拟机

MEMO

13.1 知识介绍——服务器虚拟化概述

虚拟化技术是一种资源管理技术，将一台计算机虚拟为多台逻辑计算机，每台逻辑计算机可运行不同的操作系统，并且应用程序都可以在相互独立的空间内运行而互不影响。虚拟化技术主要用来解决高性能的物理硬件和老旧硬件的重组重用，透明化底层物理硬件，从而最大化地利用物理硬件，提高计算机的工作效率，节约资源。

网络中运行着多个服务器，各服务器操作系统不同，利用率不高，例如，数据库服务器运行在 Linux 平台，邮件服务器运行在 Windows 平台，如果将所有的服务整合到一台服务器中，可大大提高资源利用率，方便管理。Windows Server 2008 R2 虚拟化解决方案就是在一台服务器上创建多个虚拟机，然后将不同的服务分别部署在不同的虚拟机上，节省了硬件的投入，所有的服务集中整合也方便了管理。除了服务器整合应用，利用 Windows Server 2008 R2 虚拟化解决方案还可以更方便地搭建测试平台，在虚拟环境下做必要测试。

Hyper-V 是 Windows Server 2008 R2 的一个功能组件，提供了基本的虚拟化平台，只要计算机的 CPU 速度够快、内存够大、硬盘容量够大，就可以创建多台虚拟机与虚拟网络。Hyper-V 的硬件需求如下。

- CPU 必须支持 64 位，计算机需要安装 Windows Server 2008 R2 或其他 64 位版本的 Windows Server 2008 及以上操作系统。
- CPU 必须支持虚拟化技术 AMD-V(AMD Virtualization)或 Intel-VT（Intel Virtualization Technology），主板 BIOS 必须启用 AMD-V 或 Intel-VT。
- 必须启用硬件数据执行保护（Data Execution Protection，DEP）。

13.2 任务 1：安装 Hyper-V

配置 Windows Server 2008 R2 服务器满足安装 Hyper-V 的所有条件，安装 Hyper-V 步骤如下所述。

STEP1 在如图 13-1 所示的“添加角色向导”窗口中选择“Hyper-V”，单击“下一步”按钮，在出现的“Hyper-V 简介”页面中再次单击“下一步”按钮。

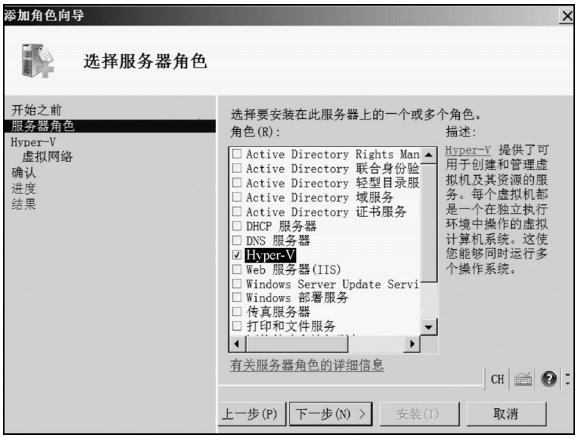


图 13-1 添加 Hyper-V 角色

STEP2 在如图 13-2 所示的“创建虚拟网络”页面中单击“下一步”按钮，稍后再创建虚拟网络连接。

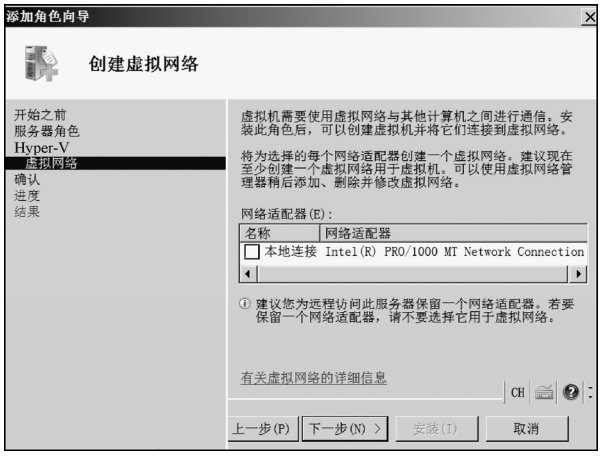


图 13-2　创建虚拟网络

STEP3 在如图 13-3 所示的“确认安装选择”页面中单击“安装”按钮，显示安装进度，安装完成后，提示重新启动计算机。

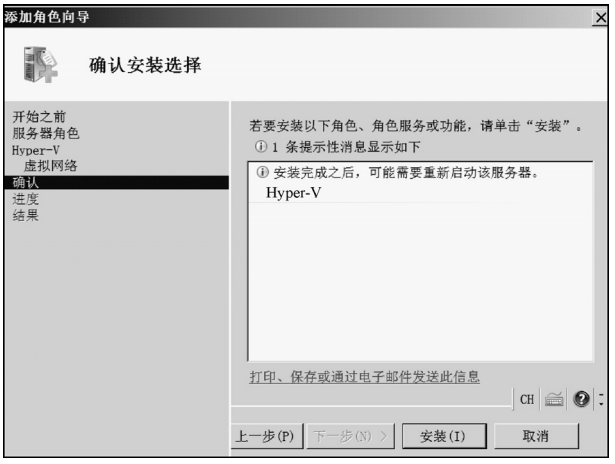


图 13-3　确认安装 Hyper-V

STEP4 重新登录系统后，自动启动服务器管理器，并继续完成后续安装任务，确认安装无误后，单击“关闭”按钮，完成 Hyper-V 安装。

13.3　任务 2：创建虚拟网络

Hyper-V 提供 3 种类型虚拟网络，有外部虚拟网络、内部虚拟网络和专用虚拟网络。

- 外部虚拟网络：是主机物理网卡连接的网络，应用外部网络的虚拟机可以与物理机所在的物理网络中其他计算机通信，可以连接 Internet。如果主机有多块物理网卡，则可以针对每一块网卡创建一个外部虚拟网络。

- 内部虚拟网络：连接在内部虚拟网络上的虚拟机之间以及虚拟机与物理机之间可以通信，但是无法与外部网络通信，无法连接 Internet。
- 专用虚拟网络：连接在专用虚拟网络上的虚拟机之间可以通信，但不能与主机通信，也无法与其他网络内的计算机通信。

STEP1 选择“开始”→“管理工具”→“Hyper-V 管理器”，打开如图 13-4 所示的 Hyper-V 管理控制台。

图 13-4　Hyper-V 管理器

STEP2 单击图 13-4 操作窗格的“虚拟网络管理器”，在图 13-5 所示的窗口选择创建虚拟网络的类型，这里选择“外部”，单击“添加”按钮。

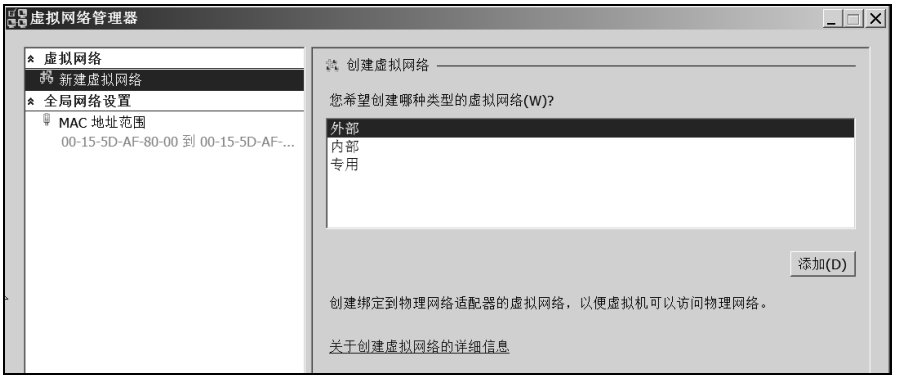


图 13-5　虚拟网络管理器（1）

STEP3 在图 13-6 中为此虚拟网络命名，并将此虚拟网络连接物理网卡。Hyper-V 会在主机内创建一块连接到此虚拟机的虚拟网卡，通过查看网络连接可以看到增加的“本地连接 3”，如图 13-7 所示。

注意：

如果要用这台虚拟机来连接 Internet，或者与此网络内的其他计算机通信，需要设置虚拟网卡“本地连接 3”的 TCP/IP 属性，而不是更改物理网卡的 TCP/IP 属性。

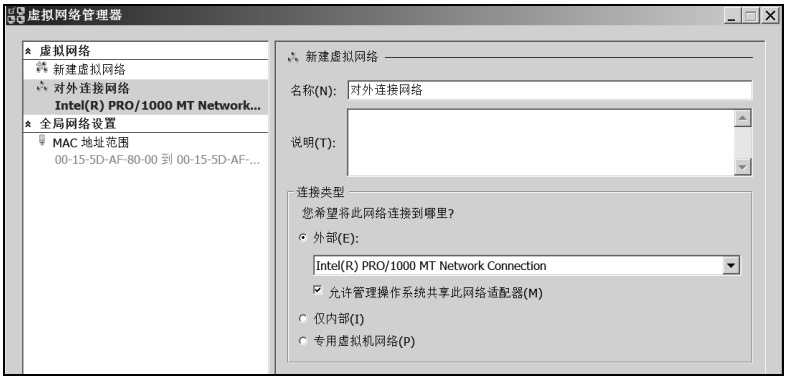


图 13-6　虚拟网络管理器（2）

图 13-7　查看网络连接

13.4　任务 3：创建虚拟机

下面将利用 Hyper-V 来创建一个虚拟机，在此虚拟机内安装 Windows Server 2008 R2 操作系统，以此作为服务器。

STEP1 打开“Hyper-V 管理器”，右键单击服务器名称，如图 13-8 所示，选择“新建”→“虚拟机”，会出现“新建虚拟机向导”窗口。

图 13-8　新建虚拟机

STEP2 在“开始之前”对话框中单击“下一步”按钮，输入虚拟机的名字并指定虚拟机存储的位置，这里采用了默认存储位置，单击“下一步”按钮，如图 13-9 所示。

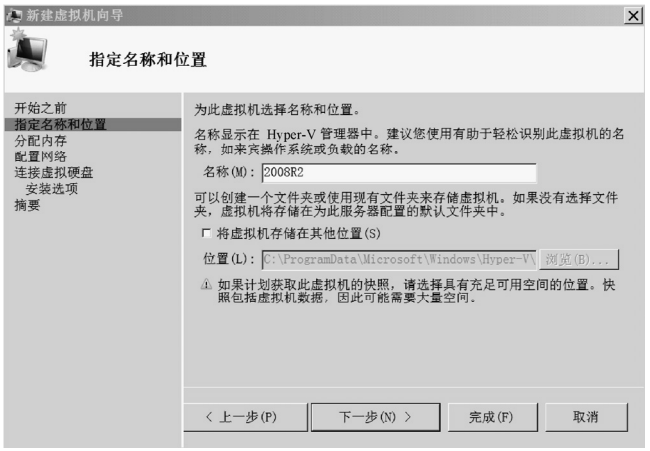


图 13-9　指定虚拟名称和存储位置

STEP3 在“分配内存”对话框中指定虚拟机内存的大小，根据要安装的虚拟机操作系统要求和物理机的内存为虚拟机分配合理内存，单击“下一步”按钮。

STEP4 在“配置网络”对话框中选择虚拟网卡所连接的网络，这里将其连接到之前创建的对外连接的网络，单击“下一步”按钮，如图 13-10 所示。

图 13-10　配置网络

STEP5 在如图 13-11 所示的“连接虚拟硬盘”对话框中设置此虚拟机的虚拟硬盘名称、存储位置、容量，单击“下一步”按钮。图中选择默认设置，创建虚拟磁盘，其容量为不固定大小的动态设置，最大可自动扩充到 127 GB。如果事先创建好了虚拟磁盘，可选择“使用现有的虚拟磁盘”并指定正确的路径。

STEP6 在如图 13-12 所示的“安装选项”对话框中选择安装方式和引导文件位置，单击“下一步”按钮。这里选择使用映像文件，也可以使用光盘和物理机的光驱引导，如果还没有准备好映像文件，可以选择“以后安装操作系统”，创建完虚拟机后，再选择引导文件。

图 13-11　设置虚拟硬盘

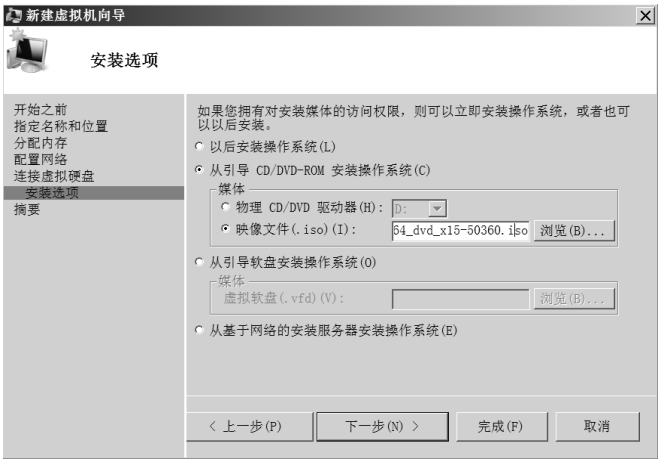


图 13-12　安装选项

STEP7 确认“正在完成新建虚拟机向导”对话框中显示的信息无误后，单击“完成”按钮，新创建的虚拟机 2008R2 如图 13-13 所示。

图 13-13　完成新建虚拟机

STEP8 双击虚拟机 2008R2，打开如图 13-14 所示的虚拟机窗口，单击工具栏上绿色的“启

动”按钮（电源）或选择“操作”→“启动”运行虚拟机。

图 13-14　虚拟机窗口

STEP9 系统开始安装 Windows Server 2008 R2（省略安装过程），如图 13-15 所示。安装过程中如果需要在虚拟机内操作鼠标，将鼠标指针移动到虚拟机窗口内，当指针变成句点图形后，单击鼠标左键。

图 13-15　安装虚拟机操作系统

注意：

鼠标要在虚拟机与物理机间随意切换或移动，需要安装 Hyper-V 集成服务。启动虚拟机操作系统，选择“操作”→“插入集成服务安装盘”，在出现的自动播放对话框中选择“安装 Hyper-V 集成服务”，安装完成后重新启动虚拟机。

13.5　任务 4：管理虚拟机

1．添加硬件

虚拟机在使用过程中有时需要增加如硬盘、网卡等硬件设备或改变内存大小、虚拟网络连接等，这些操作需要关闭虚拟机电源。右键单击图 13-13 Hyper-V 管理器中的虚拟机，选

择“设置”，打开如图 13-16 所示的虚拟机设置窗口，选择要添加的硬件，单击“添加”按钮，选择内存，可改变内存大小，选择网络适配器，可以改变虚拟网络连接类型等。

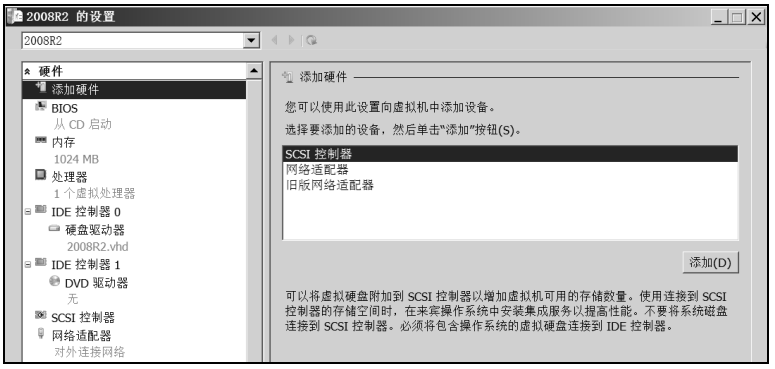


图 13-16　虚拟机设置

2．虚拟机快照

虚拟机快照能记录某个时间点虚拟机的完整状态，将虚拟机特定时刻的状态、磁盘数据和配置存为一个镜像文件，可以获取虚拟机的多个快照（甚至在其运行时），在以后的任何时间，通过快照恢复当时的实际状态。右键单击图 13-13 Hyper-V 管理器中的虚拟机，选择“快照”，建立当前虚拟机状态快照，如图 13-17 所示。

图 13-17　创建快照

3．导出 / 导入虚拟机

如果一台计算机上的虚拟机要移动到另外一台计算机上运行，可以将该虚拟机导出，然后再导入到其他计算机即可。右键单击图 13-13 Hyper-V 管理器中的虚拟机，选择“导出”，指定导出虚拟机的存放路径。在另一台计算机上的 Hyper-V 管理器窗口中，单击右侧操作窗格中的“导入虚拟机”，根据向导找到存放虚拟机的路径。

13.6 实训

实训环境

HT 公司的网络中运行着 5 台服务器，服务器利用率较低，硬件配置也已落后，公司需要集中管理所有服务器。为了节约服务器的资金投入，公司购入一台配置高、性能好的服务器，要将 5 台服务器整合到新服务器中。

需求描述

- 在新服务器上安装 Windows Server 2008 R2。
- 开启 Intel-VT 支持。
- 安装 Hyper-V 角色。
- 创建 5 个虚拟机并安装操作系统。

13.7 习题

- 对安装 Hyper-V 的计算机硬件有哪些要求？
- Hyper-V 的虚拟网络有几种类型？各种虚拟网络的用途是什么？
- Hyper-V 虚拟机可以使用哪几种虚拟磁盘？
- 查找资料，对比当前虚拟化软件的优缺点。

第 14 章

备份与灾难恢复

项目需求：

ABC 公司的文件服务器每天要向其中保存一些重要文件，希望能自动备份每天增加的文件，以便在数据损坏或丢失后能够及时恢复。另外，公司内的一些计算机经常遭受病毒或误操作等破坏而无法启动，需要做好系统备份，快速恢复系统。

技能目标：

- 理解备份的作用
- 会备份和还原数据
- 了解 Windows 高级启动选项的作用

MEMO

14.1 知识介绍——Windows 备份工具

存储在磁盘内的数据可能会因为不可抗力、人为失误和设备故障等因素而丢失，从而造成公司或个人的严重损失。只要定期备份磁盘，并将其存放在安全的地方，利用备份信息还原数据，就能尽可能减小或避免损失。

在 Windows Server 2008 R2 中，可以利用 Windows Server Backup 进行数据的备份和还原，它支持以下两种备份方式。

- 完整服务器备份：备份所有卷内的数据，即所有磁盘内的所有文件，包含应用程序和系统状态。可以使用此备份来将整台计算机还原，包括 Windows Server 2008 R2 操作系统和所有其他文件。
- 自定义备份：可以选择备份系统保留卷和一般卷（例如，C：、D：和 E：），也可以选择备份磁盘分区内指定的文件和备份系统状态等。

Windows Server Backup 还提供了以下两种选择来执行备份工作。

- 计划备份：可以制订计划，以便在指定的日期和时间自动执行备份工作，备份数据可以存储在本地磁盘、USB 或外接式磁盘和网络共享文件夹中等。
- 一次性备份：手动立即执行单次备份工作，备份数据可以存储在本地磁盘、USB 或外接式磁盘和网络共享文件夹中，如果计算机安装了 DVD 刻录机，还可以备份到 DVD 光盘内。

14.2 任务 1：备份与还原数据

14.2.1 备份数据

ABC 公司的文件服务器每天都要向其中保存一些文件，工作时间备份会影响服务器的使用，要求在下班时间自动备份。

在 Windows Server 2008 R2 中，Windows Server Backup 作为一个可选的功能组件，在默认状态下没有安装启用，因此需要添加 Windows Server Backup 功能，具体步骤如下所述。

STEP1 在“服务器管理器”窗口，单击“功能”，选择“添加功能”，在“选择功能”页面中选择“Windows Server Backup 功能”，单击“下一步”按钮，如图 14-1 所示。在出现的“确认安装选择”页面中单击“安装”按钮，显示安装进度，提示安装成功。

注意：

如果需要使用 Windows PowerShell 所提供的命令来编写脚本，以便通过此脚本来完成备份工作，请选择添加图 14-1 所示的“命令行工具”。

图 14-1　选择功能

STEP2 安装完毕后，可以在“管理工具”中打开“Windows Server Backup”工具，其主要功能界面如图 14-2 所示。Windows Server Backup 工具提供了两种备份方式 ，“备份计划”可定期自动运行备份；“一次性备份”可完成一次手动备份。

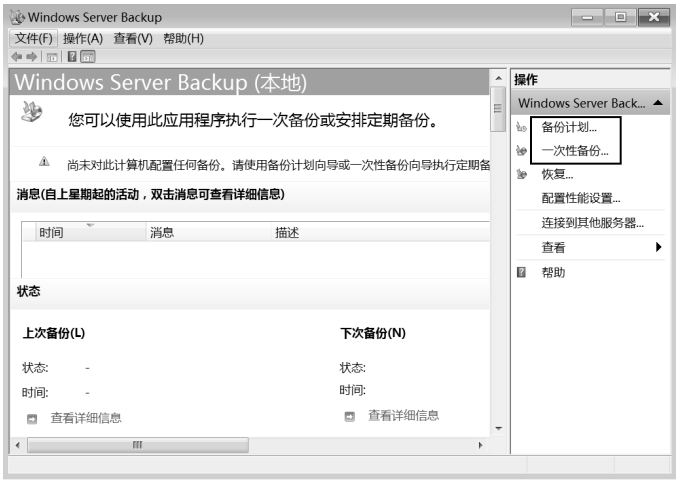


图 14-2　Windows Server Backup 窗口

STEP3 在如图 14-2 所示的“Windows Server Backup”页面右侧操作窗格中选择“备份计划”，在打开的“入门”页面单击“下一步”按钮，打开如图 14-3 所示的“选择备份配置”页面。整个服务器备份可备份所有卷内的数据，包含应用程序和系统状态。自定义备份可选择备份系统保留卷、一般卷，也可以选择备份分区内的指定文件，还可以备份系统状态，甚至可以选择裸机恢复，即备份整个操作系统，日后可以使用裸机恢复备份，还原操作系统。这里选择“自定义”，单击“下一步”按钮。

STEP4 在“选择备份的项目”页面中单击“添加项”，选择要备份的卷，如图 14-4 所示，单击“确定”，返回“选择备份的项目”页面，单击“下一步”按钮。

图 14-3　选择备份配置

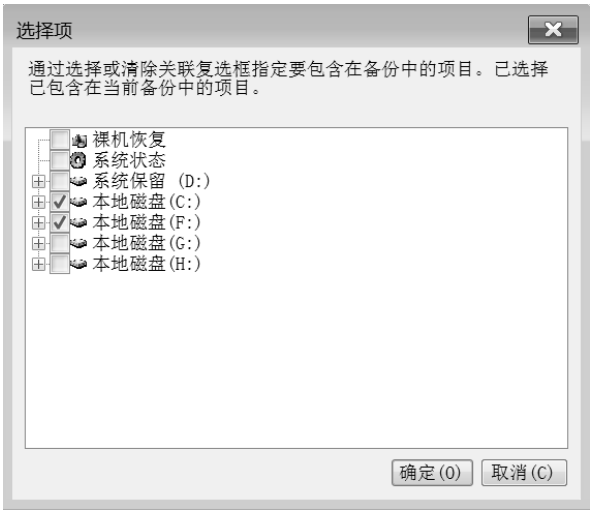


图 14-4　选择备份的项目

STEP5 在“指定备份时间”页面选择备份频率和备份时间，如希望每天特定时间备份一次，需选中“每日一次”，并设置具体时间；如希望每天多次执行备份，需选中“每日多次”，在“可用时间”列表框中选择开始时间，单击“添加”按钮。这里选择“每日一次”，并设置具体时间“21:00”，如图 14-5 所示，单击“下一步”按钮。

STEP6 在“指定目标类型”页面选择存储备份地点。“备份到专用于备份的硬盘（建议）”是最安全的备份方式，但是这种方式会将此专用硬盘格式化，因此会丢失现有数据。如果选择“备份到卷”的存储方式，卷内的数据仍然会保留，但是该卷的运行效率会降低。选择“备份到共享网络文件夹”的存储方式可以备份到网络上其他计算机的共享文件夹内。单击“下一步”按钮，如图 14-6 所示。

STEP7 在如图 14-7 所示的“选择目标磁盘”页面单击“显示所有可用磁盘”，选择目标磁盘，单击“下一步”按钮。提示备份目标磁盘将被格式化，其中现有数据将被删除，因此要备份的磁盘不可以包含目标磁盘。消息对话框如图 14-8 所示，单击“是”按钮。

图 14-5　指定备份时间

图 14-6　指定目标类型

图 14-7　选择目标磁盘

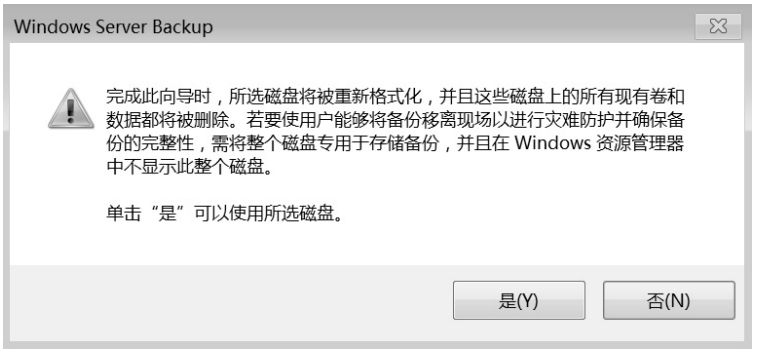


图 14-8　消息对话框

STEP8 在“确认”页面列出备份的详情，在图 14-9 的标签列可看到此备份的识别标签，日后还原时通过这个标签来识别此备份，单击“完成”按钮，打开“摘要”对话框，系统开始对目标磁盘进行格式化，格式化完毕，单击“关闭”按钮。通过以上步骤，备份计划配置完成，在每天的 21:00 将自动执行备份操作。

图 14-9　确认备份

14.2.2　还原数据

还原数据是备份数据的反向过程，将从备份文件中恢复硬盘原有文件和数据，具体步骤如下所述。

STEP1 打开“管理工具”中的“Windows Server Backup”，单击右侧窗格的“恢复”，打开“入门”页面，在“入门”页面选择备份数据的来源（存储位置），单击“下一步”按钮，如图 14-10 所示。

STEP2 在“选择备份日期”页面中，选择要恢复的备份日期和时间，如图 14-11 所示，单击“下一步”按钮。

图 14-10　选择备份存储位置

图 14-11　选择恢复的备份日期

STEP3 在“选择恢复类型”页面选择还原文件和文件夹、应用程序及卷或系统状态，如图 14-12 所示，单击“下一步”按钮。在如图 14-13 所示的“选择要恢复的项目”页面，选择要恢复的具体内容，单击“下一步”按钮。

图 14-12　选择恢复类型

图 14-13　选择要恢复的项目

STEP4 在“指定恢复选项”页面中选择“恢复目标”为“原始位置”，在“当该向导在恢复目标中已有的备份中查找项目时”对话框中选择“创建副本，以便您具有两个版本”，如图 14-14 所示，单击“下一步”按钮。在“确认”页面确认恢复信息，单击“恢复”，显示恢复进度，恢复完成后单击“关闭”按钮完成恢复操作。

图 14-14　指定恢复选项

14.2.3　备份设置

打开“管理工具”中的“Windows Server Backup”，单击右侧窗格的“配置性能设置”，将出现“优化备份性能”对话框，如图 14-15 所示。通过“优化备份性能”对话框可以针对备份性能进行高级设置。

（1）普通备份性能

创建备份的时间会与所备份的数据量成正比，这种备份方式不会降低服务器的运行性能。

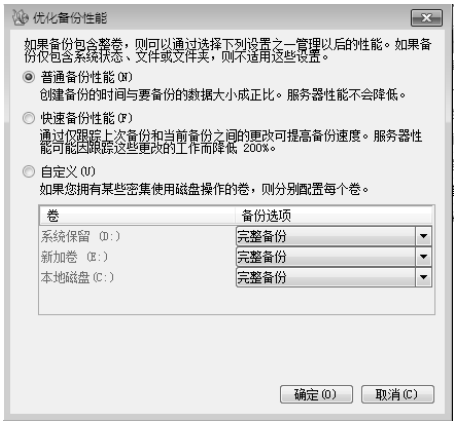


图 14-15　优化备份性能

（2）快速备份性能

所选磁盘内，只有新建的文件或有变动的文件才会被备份，以前备份过但没有再变动的文件不再备份。这种增量备份的方式，备份速度较快，但是追踪文件变动状态的操作会降低整体系统性能。

（3）自定义

可以针对不同的磁盘来选择完整备份或增量备份，完整备份用于备份所有选定的文件；增量备份仅备份上次完全或增量备份以来新增或更改的文件。

14.3　任务 2：Windows 安全模式应用

在 Windows 系统使用中，有时会因为安装了某个软件而使系统无法启动，或者在安装、升级某个硬件驱动程序后出现蓝屏。要解决这些问题，使用 Windows 安全模式会有所帮助。

要想进入安全模式，在启动计算机时按 F8 键，会出现如图 14-16 所示的“高级启动选项”页面。

图 14-16　高级启动选项

（1）修复计算机

可以进行系统还原、内存诊断和最常用的命令提示符等操作，如图 14-17 所示。

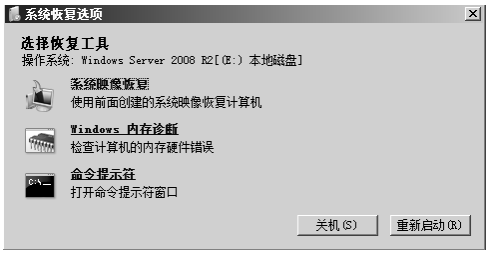


图 14-17　系统恢复选项

（2）安全模式

仅使用最基本的驱动程序启动，不支持网络功能，通过“安全模式”可以解决不能正常启动、感染病毒和账户被停用等问题。如果在系统中安装某个软件后出现了蓝屏，可以进入“安全模式”卸载软件。

（3）网络安全模式

加载了网络功能的安全模式，在启动时会加载网络设备驱动程序和网络服务，能够访问局域网和 Internet，并能从网上下载相应的修复工具和驱动程序来解决各种软件问题或因为硬件驱动程序而造成的问题。

（4）带命令提示符的安全模式

只使用基本的文件和驱动程序启动，启动后出现命令提示符界面，而非 Windows 图形界面，此模式适合 IT 专业人员。

（5）启用启动日志

在系统启动后生成一个名为 nbtlog.txt 的文件，将系统启动过程中加载和未加载的驱动程序记录到该文件中，文件 nbtlog.txt 位于%systemroot%目录。安全模式、网络安全模式和带命令提示符的安全模式会将一个加载所有驱动程序和服务的列表添加到启动日志中；启动日志可以查看系统启动存在的问题。

（6）启用低分辨率视频

使用低分辨率（640×480）启动计算机，当在安全模式下启动时，总是使用基本的视频驱动程序。

（7）最近一次的正确配置

使用 Windows 上一次关闭时所保存的注册表信息和驱动程序来启动，最后一次成功启动以来所做的任何更改将丢失。只有在当前配置不对的情况下，才使用最后一次正确的配置。但是，它不能解决由于驱动程序或文件被损坏或丢失所导致的问题。

（8）目录服务还原模式

此模式只用于恢复域控制器的系统状态，即恢复域控制器的 SYSVOL 目录和 Active Directory 目录服务。

14.4　实训

实训环境

HT 公司有一台操作系统为 Windows Server 2008 R2 的文件服务器，为防止系统出现问题，需要对服务器的系统分区进行备份，并在出现问题时进行还原。

需求描述

- 添加 Windows Server Backup 功能。
- 备份系统分区。
- 还原系统分区。

14.5　习题

- Windows Server Backup 支持哪两种备份方式？
- 在选择“备份到专用于备份的硬盘”时，要注意什么？
- Windows 高级启动选项中有哪些常用选项？
- “安全模式”启动可以解决哪些问题？
- 启动日志有什么用途？